

EAIM LIBRARY
REFERENCE SET

UNC Reg 530-1

CFC Reg 530-1

USFK Reg 530-1

Change No. 1

HEADQUARTERS

UNITED NATIONS COMMAND

UNIT #15259

APO AP 96205-0032

HEADQUARTERS

ROK-US COMBINED FORCES COMMAND

UNIT #15255

APO AP 96205-0028

HEADQUARTERS

UNITED STATES FORCES, KOREA

UNIT #15237

APO AP 96205-0010

Change #1 to

UNC/CFC/USFK Reg

No. 530-1

4 May 1998

Operations and Signal Security

OPERATIONS SECURITY (OPSEC)

HEADQUARTERS
UNITED NATIONS COMMAND
UNIT #15259
APO AP 96205-0032

HEADQUARTERS
ROK-U.S. COMBINED FORCES COMMAND
UNIT #15255
APO AP 96205-0028

HEADQUARTERS
UNITED STATES FORCES, KOREA
UNIT #15237
APO AP 96205-0010

Change No. 1
UNC/CFC/USFK Reg
No. 530-1

4 May 1998

Operations and Signal Security

OPERATIONS SECURITY (OPSEC)

1. UNC/CFC/USFK Reg 530-1, 30 July 1990, is changed as follows:

Page 1, Paragraph 3, REFERENCES. Page 1, paragraph 3a(2), insert a period after the word OPLAN and delete the remainder of the sentence from CONPLAN...6a. Replace with TAB C to Appendix 11 to Annex C of UNC, CFC, and USFK OPLAN.

Page 1, Paragraph 3, REFERENCES. Paragraph 3b(1), delete the entire sentence and replace with the following: CFC/USFK Information Operations Handbook.

Page 2, Paragraph 5, RESPONSIBILITIES. Paragraph 5c(2), at the end of the sentence after the word assistance, delete the period and add a comma and the words "as necessary."

Page 3, Paragraph 5, RESPONSIBILITIES. In paragraph 5c(5), delete the words CONPLANS, EXPLANS, and directives, and replace with "Tab C to Appendix 11 to Annex C of UNC, CFC, and USFK OPLAN."

Page 3, Paragraph 5, RESPONSIBILITIES. In paragraph 5e(1), line two, delete the words "and communications (C3)" and replace with "command and control (C2)."

Page 4, Paragraph 5, RESPONSIBILITIES. In paragraph 5g(9), line 2, change CJ-PL-CM, APO SF 96301-0010 to read CJ3-PL-IO, APO AP 96205-0010.

Page 5, Paragraph 6, GENERAL CONCEPT. Delete paragraph 6c and replace with the following:

“OPSEC is a critical component of Information Operations (IO). The IO integrates electronic warfare (EW), deception, OPSEC, Computer Network Attack (CNA), PSYOP, Public Affairs (PA), Civil Affairs (CA), and physical destruction to deny the enemy effective command and control while protecting friendly C2 from similar enemy actions. As part of IO, OPSEC preserves essential secrecy and helps to influence enemy decision makers during prehostilities. When hostilities become imminent or war starts, OPSEC protects friendly C2 capabilities, preserves the element of surprise, and increases enemy uncertainty and confusion.

Page 5, Paragraph 6, GENERAL CONCEPT. In paragraph 6e, line 1, change C3CM to read IO.

Page 6, Proponent block. In the last line of proponent block, delete “CFCD-PL-CM, APO SF 96301-0028” and replace with “CFCD-PL-IO, APO AP 96205-0010”.

Page 7, Signature page, Appendixes. Change appendix B to read “Operations Security in Support of Information Operations (IO).

Page 7, Special Distribution. In the first line, delete CFCD-PL-CM and replace with CFCD-PL-IO. Where SF’s appears, replace with AP.

APPENDIX A, Page A-2. Add paragraph A-4a(1)(f), Computer security, after paragraph A-4a(1)(e).

APPENDIX A, Page A-2. In paragraph A-4a(2), delete C3CM and replace with IO.

APPENDIX B, Page B-1. In the title, delete the words “Command, Control, and Communications Countermeasures (C3M)” and replace with “Information Operations (IO)”.

APPENDIX B, Page B-1. In paragraph B-1, lines four and five, delete C3 and replace with IO.

APPENDIX B, Page B-1. In paragraph B-2, line one, delete both C3CMs and replace with IO.

APPENDIX B, Page B-1. In paragraph B-2a, line one, delete counter-C3 and replace with offensive IO.

APPENDIX B, Page B-1. Make the following changes in paragraph B-2:

In paragraph B-2b, line one, delete C3-protect and replace with defensive IO.

In line two, delete C3 and replace with IO.

In line three, delete C3-protect and replace with defensive IO.

In line four, delete C3-protect and replace with defensive IO.

In line six, delete C3-protect and replace with defensive IO.

In line seven, delete C3 and replace with IO.

In line eight, delete counter-C3 and replace with offensive IO.

APPENDIX C, Page C-14. On page C-14, item (22), delete C3CM and replace with IO.

APPENDIX C, Page C-15. On page C-15, item b(3), delete C3CM and replace with IO.

APPENDIX C, Page C-16. On page C-16, item a(4), delete C3CM and replace with IO measures.

APPENDIX C, Page C-16. On page C-16, item b(2), delete C3CM and replace with IO.

Glossary. Make the following changes to the glossary.

Add C2W, command, and control warfare, between C2 and C3.

Delete the C3CM, command, control, and communications countermeasures.

Add C4I, command , control, communications, computers and information

Add IO, information operations, after IAW, in accordance with.

Add IW, information warfare, after IO, information operations.


2. Post these changes per DA Pam 25-40.

3. File this change in front of the publication.

Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander in Chief, UNC/CFC, ATTN: CFCD-PL-IO, APO AP 96205-0028.

FOR THE COMMANDER IN CHIEF, UNC/CFC, AND THE COMMANDER, USFK:

OFFICIAL:
RANDOLPH W. HOUSE
Lieutenant General, USA
Chief of Staff


KIM, YOUNG KYU
Colonel, ROK Army
Adjutant General, UNC/CFC


JOHN A. HALL
Assistant Adjutant General

SPECIAL DISTRIBUTION:

25 - CFCD-PL-IO
2 - SJS
4 - USAFK/7AF, APO AP 96570-5000
2 - USNFK
2 - EAIG
1 - PAJ
1 - SJA
5 - ACofS, J2
5 - ACofS, J3
5 - ACofS, J5
5 - ACofS, J6
1 - USA Special Security Command, Pacific
1 - USA Field Station-K, APO AP 96271-0161
15 - CFA, APO AP 96385-0210
15 - 2ID, APO AP 96224-0289

5 - 17th Avn Bde
2 - CSCT #1, APO AP 96397-0247
2 - CSCT #3
15 - 1st Signal Bde
4 - 501st MI Bde
1 - DCA-K
2 - CG, FMFPAC, Camp H.M. Smith, HI, APO AP 96861-5000
2 - Hq 5th AF, APO AP 96328-5000
2 - ROKAF CAC
15 - TROKA
2 - ROK MC HQ
5 - SCS
5 - ACofS, C2
5 - ACofS, C3
5 - ACofS, C5
5 - ACofS, C6
1 - USTRANSCOM LNO
1 - CFPA
2 - CFOA
2 - ACC, APO AP 96570-5000
2 - NCC, Chinhae, Korea
2 - UNCMAC, Secretariat
2 - Spec Adv UNCMAC
2 - Spec Adv CINCUNC
2 - Hq UNC, Rear, Camp Zama, Japan, APO AP 96343-0051
15 - FROKA
2 - ROK JCS
4 - Hq ROKA
4 - Hq ROKN
4 - Hq ROKAF
1 - US Joint Staff/J3, Washington, DC 20301-5000
4 - CINSEVENTHFLT, FPO FP 96601-5000
2 - USCINCPAC, Camp H. M. Smith, Hawaii, APO AP 96858-5000
2 - WESTCOM, Fort Shafter, HI APO AP 96858-5000
2 - HQ Pacific Air Force, Hickam AFB, HI, APO AP 96853-5000
2 - HQDA, EUSA LNO, DACS, EUSA-CS-SA, Washington, DC 20301-5000
2 - USCINCPACFLT, Pearl Harbor, HI 96818-5000
2 - CG, III MAF, FPO FP 96606-5000
5 - CUWTF
2 - ROKA Aviation Hq
3 - AMXFE
90 - USA PPCK
8 - EAIM-R-PM (Editing)

UNC Reg 530-1
유엔사 규정 530-1

CFC Reg 530-1
연합사 규정 530-1

USFK Reg 530-1
주한미군 규정 530-1

HEADQUARTERS
유엔사

UNITED NATIONS COMMAND
사령부

APO SAN FRANCISCO 96301-0032
군우 샌프란시스코 96301-0032

HEADQUARTERS
한-미 연합사

ROK-US COMBINED FORCES COMMAND
사령부

SEOUL, KOREA
서울, 한국

APO SAN FRANCISCO 96301-0028
군우 샌프란시스코 96301-0028

HEADQUARTERS
주한미군

UNITED STATES FORCES KOREA
사령부

APO SAN FRANCISCO 96301-0010
군우 샌프란시스코 96301-0010

UNC/CFC/USFK Regulation
유엔사/연합사/주한미군 규정

No. 530-1
번호. 530-1

30 July 1990

1990년 7월 30일

(Effective Date 30 August 1990)
Operations and Signal Security
작전 및 신호 보안

OPERATIONS SECURITY (OPSEC)
작전 보안

HEADQUARTERS
UNITED NATIONS COMMAND
APO SAN FRANCISCO 96301-0032

HEADQUARTERS
ROK-US COMBINED FORCES COMMAND
SEOUL, KOREA
APO SAN FRANCISCO 96301-0028

HEADQUARTERS
UNITED STATES FORCES KOREA
APO SAN FRANCISCO 96301-0010

UNC/CFC/USFK Regulation
No. 530-1

30 July 1990

(Effective Date 30 August 1990)
Operations and Signal Security
OPERATIONS SECURITY

SUPPLEMENTATION. Issue of further supplements to this regulation by subordinate commands is prohibited unless prior approval is obtained from HQ UNC/CFC, ATTN: CFCD-PL-CM, APO SF 96301-0028.

1. **PURPOSE.** This regulation provides operations security (OPSEC) policy and guidance for United Nations Command (UNC), Combined Forces Command (CFC), and United States Forces Korea (USFK) components and subordinate commands and staffs.

2. **APPLICABILITY.** This regulation applies to all personnel and units assigned and attached to, under operational control of, or in support of UNC, CFC, or USFK.

3. **REFERENCES.**

a. The following are required publications:

- (1) AFR 55-30 (Operations Security). Cited in subparagraph 5g(10).
- (2) Appendix 1 to Annex L of UNC, CFC, and USFK OPLAN, CONPLAN, and OPORD (S-ROKUS). Cited in subparagraph 6a.
- (3) AR 530-1 (Operations Security (OPSEC)). Cited in subparagraph 5g(10).
- (4) Tri-Service Agreement. Cited in subparagraph 8b.

b. The following are related publications:

- (1) CFC/USFK Command, Control, and Communications Countermeasures (C3CM) Handbook.

***This regulation supersedes UNC/CFC Reg 530-1, 23 June 1980.**

- (2) JCS Pub 3-54 (Joint Doctrine for Operations Security).
- (3) J3M-947-83 (OPSEC Survey Guide).
- (4) OPNAVINST 3070.1A (Operations Security).

4. EXPLANATION OF ABBREVIATIONS. Abbreviations used in this regulation are explained in the glossary.

5. RESPONSIBILITIES.

a. Each Assistant Chief of Staff (ACofS) and special staff section will establish an OPSEC program within its divisions, branches, and sections to emphasize the importance of OPSEC. Specific staff responsibilities are established in subparagraphs b through i below. As a minimum, each ACofS and special staff section will--

- (1) Designate an OPSEC officer, preferably at the O4-level or above, in the operations/plans section. This officer will be the staff's OPSEC representative and participate in the CFC/USFK OPSEC Working Group.

- (2) Identify, prioritize, and develop measures to protect indicators that might provide the enemy with foreknowledge of CFC/USFK operations and capabilities.

- (3) Respond to CFC/USFK OPSEC Officer taskings.

b. The UNC/CFC/USFK, ACofS, C/J2, will--

- (1) Assist the ACofS, C/J3, in developing essential elements of friendly information (EEFI).

- (2) Identify deception opportunities.

- (3) Provide input to and review deception plans as necessary. Conduct deception tasks as required.

- (4) Maintain hostile intelligence collection threat data base.

- (5) Analyze threat collection capabilities and intentions.

- (6) Assist in developing friendly force profiles.

- (7) Identify friendly force vulnerabilities to intelligence collection, terrorism, and sabotage.

c. The UNC/CFC/USFK, ACofS, C/J3, will--

- (1) Designate the CFC/USFK OPSEC officer in the ACofS, C/J3, Plans Division.

- (2) Budget for OPSEC activities to include operations, exercises, OPSEC surveys and evaluations, training, and assistance.

(3) Provide OPSEC management, planning, and execution guidance to component and subordinate commands and staff.

(4) Coordinate OPSEC concerns with the Republic of Korea (ROK) Ministry of National Defense and appropriate Department of Defense agencies.

(5) Prepare the OPSEC annex for CFC/USFK OPLANS, CONPLANS, EXPLANS, and directives.

d. The UNC/CFC/USFK, ACoS, C/J4, will analyze logistics reports and procedures to identify indicators compromising CFC/USFK intent.

e. The UNC/CFC/USFK, ACoS, C/J6, will--

(1) Assist the ACoS, C2, and ACoS, C3, in developing the command, control, and communications (C3)-protect appendix for CFC/USFK OPLANS, CONPLANS, and exercise directives.

(2) Establish emission control and wartime reserve modes for CFC/USFK communication emitters.

f. The UNC/CFC/USFK, ACoS, Engineer, will--

(1) Provide technical advice on construction as it applies to camouflage and deception features at fixed installations and facilities.

(2) As requested, ensure counter-surveillance measures are incorporated in the design and construction of fixed installations and facilities.

g. Components and subordinate commands will--

(1) Designate an OPSEC officer within the operations staff. This officer will be the command's OPSEC representative on the CFC/USFK OPSEC Working Group.

(2) Form a unit level OPSEC working group. Unit staffs must participate actively in the unit program and working group.

(3) Budget for OPSEC activities on an annual basis.

(4) Prepare OPSEC annexes to OPLANS, EXPLANS, CONPLANS, and exercise directives.

(5) Develop a subordinate unit and staff OPSEC training program.

(6) Provide subordinates OPSEC planning and execution guidance.

(7) Provide CFC/USFK OPSEC Survey Team augmentation, as required.

(8) Develop unit EEFI. Review on an annual basis.

(9) Conduct an OPSEC survey biennially. Forward requests for external assistance to the Commander, USFK, ATTN: CJ-PL-CM, APO SF 96301-0010.

(10) Submit the annual OPSEC activities report (OPSEC REP: RCS JCS-OY) to the UNC/CFC/USFK OPSEC Officer not later than (NLT) 15 July (ref AR 530-1, para 1-10). Format will be provided by message from CFC/USFK NLT 15 June. The 7th United States Air Forces Korea (USAFK) will submit the report in accordance with (IAW) AFR 55-30 and PACAF directives.

(11) Develop unit profiles as a long-term effort.

h. The UNC/CFC/USFK OPSEC Officer will--

(1) Receive taskings from the ACoS, C/J3.

(2) Task (for the commander through the C/J3) subordinate units to conduct necessary OPSEC surveys and evaluations.

(3) Foster joint combined OPSEC capabilities development.

(4) Establish a CFC/USFK OPSEC Working Group.

(5) Develop the UNC/CFC/USFK OPSEC Long-Range Plan.

(6) Chair the UNC/CFC/USFK Working Group.

(7) Supervise OPSEC surveys of critical CFC/USFK activities.

(8) Submit the USFK annual OPSEC activities report (OPSEC REP: RCS JCS-OY) to the USCINCPAC NLT 1 August.

i. The CFC/USFK OPSEC Working Group will meet, as required, to--

(1) Review and coordinate OPSEC program directives and initiatives.

(2) Review command OPSEC and staff survey reports to identify trends, indicators, patterns, and profiles of intelligence value.

(3) Develop methods to improve UNC/CFC/USFK OPSEC posture.

(4) Recommend countermeasures and deception tactics to protect vulnerable indicators.

(5) Evaluate open source publications having an OPSEC impact on the command's mission.

(6) Provide command emphasis for OPSEC activities.

(7) Recommend operations requiring OPSEC evaluations and surveys.

6. GENERAL CONCEPT.

a. Operations security is the process of denying the enemy critical information about friendly capabilities and intentions. The process includes identifying, controlling, and protecting indicators associated with military operations and other activities. Indicators provide the critical information, classified or unclassified, the enemy needs to counter UNC/CFC/USFK intentions and undermine effectiveness. Appendix 1 to annex L of UNC, CFC, and USFK OPLAN, CONPLAN, and OPORD (S-ROKUS) identifies the command's critical information.

b. Operations security is broad in scope and depends upon collecting intelligence, adhering to the traditional security disciplines, and analyzing staff functions to identify, control, and protect indicators.

c. OPSEC is a critical component of command, control, and communications countermeasures (C3CM). C3CM integrates electronic warfare, deception, OPSEC, and physical destruction to deny the enemy effective command and control while protecting friendly C3 from similar enemy actions. As part of C3CM, OPSEC preserves essential secrecy and helps to influence enemy decision makers during prehostilities. When hostilities become imminent or war starts, OPSEC protects friendly C3 capabilities, preserves the element of surprise, and increases enemy uncertainty and confusion.

d. Deception supports military operations by simultaneously conveying and denying critical information to hostile intelligence. Depending upon the objective, deception can be used in support of OPSEC or be supported by OPSEC. When OPSEC supports deception it minimizes or eliminates indicators of friendly intent. Conversely, deception can be applied as an OPSEC countermeasure when other counter-surveillance and security techniques are unavailable or inadequate. Although OPSEC can be applied without deceptive intent, deception cannot succeed without effective OPSEC support.

e. The UNC/CFC/USFK OPSEC Officer is located in C3CM Branch, C/J3 Plans Division. This individual manages the UNC/CFC/USFK OPSEC Program and works with staffs; the Commander in Chief, Pacific (CINCPAC); the Joint Chiefs of Staff; and component and subordinate command OPSEC officers.

f. The UNC/CFC/USFK OPSEC Program has three goals. The first is to reduce the number of critical information sources available to the enemy. The second is to foster enemy misperceptions of ROK/United States (US) intent, objectives, and capabilities. The third is to develop feasible alternatives to methods of operation which may disclose UNC/CFC/USFK intent.

7. UNC/CFC/USFK OPERATIONS SECURITY POLICY.

a. Essential secrecy about UNC/CFC/USFK intentions and military capabilities is a vital concern. Effective OPSEC preserves essential secrecy and provides commanders the means to achieve surprise and retain the initiative.

b. Practice sound OPSEC every day in all activities, not just during exercises.

c. OPSEC is a command/leadership responsibility. Component and subordinate commanders and staff section chiefs will use appropriate OPSEC measures daily to preserve essential secrecy. Leaders will consider OPSEC in every phase of an activity, exercise, or operation. Standard staff operational procedures, reports, and routines can inadvertently reveal vulnerabilities. Conscious, planned staff implementation of effective OPSEC measures is crucial to the OPSEC process.

d. Although the operations staff element has primary staff responsibility for OPSEC, commanders and staff chiefs must ensure that all subordinate commanders and staff elements integrate OPSEC in all procedures and planning processes.

8. OPSEC SUPPORT AND SERVICES.

a. The 501st Military Intelligence Brigade provides--

(1) Threat assessment and risk analysis of designated communications systems as directed by the ACoFS, J2/J3.

(2) Cryptofacility inspections for accounts holding keying material under the controlled communications security (COMSEC) items program to determine overall security status and identify/analyze discrepancies and impact on COMSEC materials protection.

(3) Technical surveillance countermeasures surveys to detect technical surveillance devices, hazards, and physical security weaknesses.

b. The 6903 Electronic Security Group provides COMSEC monitoring and analysis support to 7th USAFK subordinates. Activities include both telephone and radio monitoring. District 45 Office of Special Investigations provides requested technical services to Air Force units IAW the Tri-Service Agreement.


<p>The proponent of this regulation is the Office of the Assistant Chief of Staff, C3. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander in Chief, UNC/CFC, ATTN: CFCD-PL-CM, APO SF 96301-0028.</p>


FOR THE COMMANDER IN CHIEF, UNC/CFC, AND THE COMMANDER, USFK:

JAMES F. RECORD
Major General, USAF
Chief of Staff, UNC/CFC

OFFICIAL:

JAMES R. TAYLOR
Major General, USA
Chief of Staff, USFK


CHOI, YOUNG CHOL
Lieutenant Colonel, ROK Army
Adjutant General, UNC/CFC


GEORGE F. REAVES
Lieutenant Colonel, USA
Assistant Adjutant General, USFK

3 Appendixes

- A. Operations Security Training
- B. Operations Security in Support of
Command, Control, and Communica-
tions Countermeasures (C3CM)
- C. Operations Security Indicators

Glossary

SPECIAL DISTRIBUTION:

- 25 - CFCD-PL-CM
- 2 - SJS
- 4 - USAFK/7AF, APO SF 96570-5000
- 2 - USNFK
- 3 - JUSMAG-K, APO SF 96302-0187
- 2 - EAIG
- 1 - PAJ
- 1 - SJA
- 5 - ACoS, J2
- 5 - ACoS, J3
- 2 - ACoS, J5
- 8 - ACoS, J6

1 - USA SPECIAL SECURITY CMD, PACIFIC
 1 - USA FIELD STATION-K, APO SF 96271-0161
 15 - CFA, APO SF 96385-0210
 15 - 2ID, APO SF 96224-0289
 5 - 17th AVN BDE
 2 - CSCT #1, APO SF 96397-0247
 2 - CSCT #3
 15 - 1st SIGNAL BDE
 4 - 501st MI BDE
 1 - DCA-K
 2 - CG, FMFPAC, CAMP H. M. SMITH, HI, APO SF 96861-5000
 2 - HQ 5AF, APO SF 96328-5000
 2 - ROKAF CAC
 15 - TROKA
 2 - ROK MC HQ
 5 - SCS
 5 - ACoS, C2
 5 - ACoS, C3
 5 - ACoS, C5
 5 - ACoS, C6
 1 - USTRANSCOM LNO
 1 - CFPA
 2 - CFOA
 2 - ACC, APO SF 96570-5000
 2 - NCC, CHINHAE, KOREA
 2 - UNCMAC SECRETARIAT
 2 - SPEC ADV UNCMAC
 2 - SPEC ADV CINCUNC
 2 - HQ UNC, REAR, CAMP ZAMA, JAPAN, APO SF 96343-0051
 15 - FROKA
 2 - ROK JCS
 4 - HQ ROKA
 4 - HQ ROKN
 4 - HQ ROKAF
 1 - US JOINT STAFF/J3, WASHINGTON, DC 20301-5000
 4 - COMSEVENTHFLT, FPO SF 96601-5000
 2 - USCINCPAC, CAMP H. M. SMITH, HI APO SF 96858-5000
 2 - WESTCOM, FORT SHAFTER, HI, APO SF 96858-5000
 2 - HQ PACIFIC AIR FORCE, HICKAM AFB, APO SF 96853-5000
 2 - HQDA EUSA LNO DACS EUSA-CS-SA, WASHINGTON, DC 20301-5000
 2 - USCINCPACFLT, PEARL HARBOR, HI 96818-5000
 2 - CG, III MAF, FPO SF 96606-5000
 5 - CUWTF
 2 - ROKA AVIATION HQ
 3 - AMXFE
 90 - USA PPCK 96483-0121
 8 - FJ-PRM-P

APPENDIX A

OPERATIONS SECURITY TRAINING

A-1. GENERAL. Unit leaders and OPSEC officers are responsible for planning and conducting OPSEC training. OPSEC training requires a common sense approach since, at its basic level, OPSEC translates into the survival of the soldier on the battlefield. Leaders and OPSEC officers integrate OPSEC with other training activities to preserve essential training time.

A-2. OBJECTIVES.

a. Unit training programs have two objectives: Threat awareness and secure performance.

b. Threat awareness training educates individuals about operations, capabilities, and techniques of enemy hostile intelligence collectors.

c. Secure performance training teaches individuals how to do their jobs under the most secure measures, thus neutralizing the enemy's intelligence collection effort. Leaders and OPSEC officers conduct this training in multiple phases to focus on specific needs of targeted personnel.

A-3. THREAT AWARENESS TRAINING.

a. Effective threat awareness training is tailored to the unit's specific mission. In addition, the training considers the enemy's intelligence collection capabilities, techniques, and limitations. Threat Awareness Training must be as current and factual as security constraints and information availability permit.

b. Unit OPSEC officers coordinate with the intelligence staff officers and the ACoFS C/J2 to obtain the most current hostile intelligence threat information and briefing material.

A-4. SECURE PERFORMANCE TRAINING.

a. Phase 1 training ensures all unit personnel understand OPSEC principles and how OPSEC relates to other traditional security programs. All unit personnel receive this training within 30 days of arrival in-country. Refresher training, which reinforces the cause and effect relationship between everyday activities and enemy intelligence collection efforts, is essential. Phase 1 topics include--

- (1) OPSEC's relationship to other security programs.
- (a) Information security.
- (b) COMSEC.

- (c) Electronics security.
- (d) Physical security.
- (e) Emission control.
- (2) OPSEC's relationship to tactical deception and C3CM.
- (3) Camouflage and countersurveillance training, to include--
 - (a) Individual camouflage techniques.
 - (b) Use of shadows, terrain, and natural camouflage to conceal military equipment.
 - (c) Proper employment of camouflage nets.
 - (d) Proper dispersal of vehicles and equipment.
 - (e) Noise, light, and litter discipline.
 - (f) Development of unit track plans.
- (4) Counter-Signals Intelligence training, to include--
 - (a) Net control.
 - (b) Proper telephone techniques.
 - (c) Authentication procedures.
 - (d) Electronic security techniques.
 - (e) Manual crypto procedures.
 - (f) Proper use of radio frequencies and call-signs.
 - (g) Proper antenna setting.
 - (h) Proper use of radio silence.
 - (i) Minimum power use for radio/radar transmitters.
 - (j) Alternate means of communication.
 - (k) Brevity list procedures.
 - (l) Radio maintenance procedures.
 - (m) Cryptographic key procedures.

- (5) Information security training, to include--
 - (a) Proper handling and transfer of classified material.
 - (b) Classification guidance.
 - (c) Destruction of classified materials.
 - (d) Reproduction of classified materials.
- (6) Physical security training, to include--
 - (a) Selecting command post and assembly areas.
 - (b) Establishing security perimeters.
 - (c) Challenge and password procedures.
 - (d) Selecting dismount points and vehicle parks.
 - (e) Individual search procedures.

b. Phase 2 training is for personnel who are directly or indirectly engaged in classified or sensitive activities. Phase 2 training objectives are developing the capability to recognize specific intelligence indicators associated with duties and understanding how these indicators reveal EEFI. Once identified, personnel must also learn how to protect these indicators. Indicators will vary depending on the specific activity or operation, but will fall generally into two broad categories; unit capabilities and system development, test and evaluation capabilities indicators. Potential indicators are--

- (1) Capabilities indicators.
 - (a) Observable training and exercise activities which involve new weapons, equipment, aircraft, procedures, and doctrines.
 - (b) Reaction to exercise or actual hostile actions.
 - (c) Spare parts availability.
 - (d) Reports indicating the state of training and experience of personnel.
 - (e) Reports which address the adequacy of numbers of personnel in key specialities.
 - (f) Visits of special repair and maintenance teams or civilian technical representatives.

- (g) Activity to install, modify, or repair systems and facilities.
- (h) Equipment checkout after takeoff.
- (i) Maintenance brevity codes.
- (j) Success or failure of unit evaluations or exercises.
- (k) Construction and repair requirements.
- (l) Reports of adverse maintenance trends.
- (2) Systems development, test and evaluation capabilities indicators.
- (a) Emissions during tests and exercises.
- (b) Technical journals and reports.
- (c) Budgets.
- (d) Systems themselves.
- (e) Schedules of upcoming tests and exercises.
- (f) Deployment of units and sensor systems to support tests.
- (g) Security imposed on particular developments.
- (h) Special manning for tests.
- (i) Notices to mariners and airmen.
- (j) Stereotyped procedures and sequences of actions in test preparation.

c. Phase 3 training is for staff planners. Staff planners must identify, control, and eliminate indicators as they develop unit plans, orders, and directives. Staff planners also require a fundamental understanding of enemy intelligence collection capabilities and a thorough understanding of OPSEC principles. Training will focus on comparing normal activity with activity expected during a planned operation or activity. Planners must consider--

- (1) How is the indicating action, unit, object, or person involved with the operation? What is the normal activity apart from operations?
- (2) Where is the indicating action, unit, object, or person observed when involved with the operation? Where is it normally observed?
- (3) When is the indicating action first involved with the operation? What is normal involvement?

(4) How much of the indicating action is involved with the operation? How much would normally be involved in routine activities?

(5) How many indicating actions are involved? How many would normally be involved in routine activities?

(6) How many times is the indicating action involved? How many times is the action normally involved in activities outside of operations?

(7) What is different, unusual, or distinct about the involvement compared with normal activity?

(8) What are the changes in, about, or around these departures from normal activity? Do the differences and the changes surrounding them become operations indicators?

d. Phase 4 training is for senior officers and commanders. These individuals must understand the importance of surprise and how to achieve it in their operations. Further, they need to understand how OPSEC contributes to this objective and its relationship to operational effectiveness.

APPENDIX B

OPERATIONS SECURITY IN SUPPORT OF COMMAND, CONTROL, AND COMMUNICATIONS COUNTERMEASURES (C3CM)

B-1. GENERAL. All military forces, regardless of size, require some form of command and control (C2) to accomplish their mission. Normally, this C2 closely relates to and depends on communications. Commanders can greatly increase their chances of success if they can disrupt the enemy's C3 while simultaneously protecting their own C3 systems.

B-2. OPSEC IN SUPPORT OF C3CM. An effective C3CM strategy must provide long-term denial of critical information to enemy planners. Allowing the enemy to make plans based on complete, accurate information minimizes enemy communications requirements during an engagement. This reduces the US's opportunity to either exploit enemy communications or disrupt the decision cycle through destruction, jamming, or deception.

a. In support of counter-C3, an effective OPSEC program cuts off critical tactical and strategic information. Decision errors in combat can be deadly. Wrong decisions can result in the wrong force in the wrong place at the wrong time. As the battle develops, the enemy is forced to exchange information, modify plans, and redirect forces. The increasing need to exchange information provides further opportunities to degrade enemy C2 through jamming, deception, or destruction.

b. In support of C3-protect, OPSEC provides the essential secrecy to critical C3 nodes, network structures, and operational frequencies. At the strategic level, effective C3-protect is a valid concern to operational research, test, and development functions. Effective C3-protect can prevent the enemy from learning about a new weapon system and afford the element of technical surprise. Poorly planned and executed C3-protect can result in operational deficiencies reducing operational effectiveness when friendly C3 systems become targets for enemy counter-C3.

APPENDIX C

OPERATIONS SECURITY INDICATORS

C-1. COMMON INDICATORS.

- a. Indicators establishing profiles.
 - (1) Access lists.
 - (2) Availability.
 - (3) Conferences and meetings.
 - (4) Coordination.
 - (5) Readiness rating factors.
 - (6) Data processing requirements.
 - (7) Fixed sequence of actions.
 - (8) Hours of operation.
 - (9) Identifiers.
 - (a) Abbreviations/acronyms.
 - (b) Codewords.
 - (c) Mission designators.
 - (d) Nicknames.
 - (e) Project numbers.
 - (10) Implementing/execution procedures.
 - (11) Inspection/evaluation/test results.
 - (12) Interagency/international agreements.
 - (13) Limiting factors.
 - (14) Locations of units/resources.
 - (15) Missions assigned.
 - (16) Nuclear weapons procedures.

- (17) Orders.
 - (18) Performance criteria.
 - (19) Personnel assigned/staff composition.
 - (20) Proficiency.
 - (21) Quality control.
 - (22) Reports/reporting.
 - (23) Requirements.
 - (24) Restrictions.
 - (25) Security checks and tests.
 - (26) Security clearance requirements.
 - (27) Signature features (activities/materials).
 - (28) Spontaneous reactions and timing.
 - (29) Standard (fixed) operating procedures.
 - (30) State of readiness.
- b. Indicators showing deviations.
- (1) Augmentation.
 - (2) Backup resources/procedures.
 - (3) Convening special groups/staffs.
 - (4) Critical timing.
 - (5) Deficiencies/breakdowns.
 - (6) Distinguishing emblems and logos.
 - (7) Efficiency measures.
 - (8) Emergency procedures.
 - (9) Exercise/rehearsals.
 - (10) Homemade codes.

- (11) Intensity of activity.
- (12) Key words.
 - (a) Critical.
 - (b) Higher headquarters.
 - (c) Priority.
 - (d) Rush.
 - (e) Special.
- (13) Locations.
 - (a) Origins/destinations.
 - (b) Pre-positioned assets.
 - (c) Units/resources.
- (14) Planning conferences.
- (15) Priorities assigned.
- (16) Priorities of services.
- (17) Requirements changes.
- (18) Rush requirements.
- (19) Security awareness and alertness.
- (20) Security clearance requirements.
- (21) Security enhancements.
- (22) Shortages and limitations.
- (23) Special requirements.
- (24) Times/dates.
 - (a) Arrival/departure.
 - (b) Milestone.
 - (c) Suspense.

- (d) Timeliness.
- (25) Volume of services requested/provided.
- (26) Violations of security.

C-2. ADMINISTRATION ACTIVITY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Accountability records.
 - (2) Administrative organization.
 - (3) Clerical workload.
 - (4) Distribution/address indicating group lists.
 - (5) Document receipts.
 - (6) Job and position descriptions.
 - (7) Mail volume.
 - (8) Mission statements.
 - (9) Operational organization.
 - (10) OPLAN/OPORDER numbers.
 - (11) Property/inventory receipts.
 - (12) Publication volume/priorities.
 - (13) Security classification.
 - (14) Security classification guides.
 - (15) Tables of organization and equipment (TOE), tables of distribution and allowance (TDA), modified TOE, and standing operating procedures.
- b. Indicators showing deviations.
 - (1) Accident/incident/mishap reports.
 - (2) Administrative correspondence.
 - (3) Forms requests.
 - (4) Mail address changes.

- (5) Mail forwarding.
- (6) Report distribution.
- (7) Security clearance requests.
- (8) Security investigations.
- (9) Work orders/job requests.

C-3. PERSONAL AFFAIRS INDICATORS.

a. Indicators establishing profile.

- (1) Apparel.
- (2) Child care services.
- (3) Education program participation.
- (4) Immunization records.
- (5) Laundry services.
- (6) Newspaper delivery.
- (7) Passport.
- (8) Personal equipment.
- (9) Personal plans.
- (10) Personal routine.
- (11) Personal vehicle identification.
- (a) Post sticker.
- (b) Job related bumper stickers.
- (c) License plates.
- (d) Parking permits.
- (12) Physical examinations/tests.
- (13) Purchase of personal effects.
- (14) Security clearance/accesses.

- (15) Spouse/dependent affairs and routines.
- (16) Telephone services/directory listing.
- (17) Unit patches, special insignia.
- b. Indicators showing deviations.
 - (1) Advance payments.
 - (2) Billeting.
 - (3) Car rental.
 - (4) Changes of address.
 - (5) Check-in/check-out of government housing.
 - (6) Hotel/motel reservations.
 - (7) Mail forwarding.
 - (8) Permanent change of station orders.
 - (9) Personal arrangements for dependents.
 - (10) Personal arrangements for property care.
 - (11) Personal luggage.
 - (12) Powers of attorney.
 - (13) Sale/purchase/rental of residence.
 - (14) Security investigation.
 - (15) Temporary duty orders.
 - (16) Termination of leave.
 - (17) Travel authorizations/vouchers.
 - (18) Use of commercial transportation.
 - (19) Wills.

C-4. PERSONNEL ACTIVITY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Military occupational specialty (MOS) requirements.
 - (a) Assigned strengths/shortage by grade.
 - (b) By unit, TDA.
 - (c) By critical shortage in MOS.
 - (d) Shortages.
 - (2) Unit status.
 - (3) Apparel.
 - (4) Billeting arrangements.
 - (5) Unit testing.
 - (6) Unit proficiency.
 - (7) Equipment/skill/relationship.
 - (8) Manpower strength and projections.
 - (9) Medical/dental care routine.
 - (10) Morale and discipline.
 - (11) Name tags.
 - (12) Personnel activity.
 - (13) Personnel duty schedules.
 - (14) Personnel identities.
 - (15) Personnel locations.
 - (16) Retention/reenlistment.
 - (17) Security investigations.
 - (18) Specialized personnel.
 - (19) Staff officer assignments.

- (20) State of training.
- (21) Qualification skills.
- (22) Training.
- (23) Unit patches.
- (24) Unit strength.
- b. Indicators showing deviations.
 - (1) Casualty reports.
 - (2) Deployment orders.
 - (3) Education program modifications.
 - (4) Immunization requirements/records.
 - (5) Mobility processing.
 - (6) Off-limits areas.
 - (7) Personnel assembly.
 - (8) Personnel hirings/layoffs.
 - (9) Personnel notifications.
 - (10) Personnel recall.
 - (11) Physical examinations/tests.
 - (12) Skill shortages.
 - (13) Small arms possession.
 - (14) Special manning.
 - (15) Special skill requirements.
 - (16) Special team deployment/visit.
 - (17) Survival training.
 - (18) Tailored training.
 - (19) TDY funds.

- (20) Termination of leave.
- (21) Travel authorizations/vouchers.
- (22) Travel reservations.
- (23) Unfavorable personnel informations/actions.
- (24) Unit activation.
- (25) Unit alerts.

C-5. SCHEDULES. Schedules serve to establish profiles of normal activity and also may identify deviations from normal profiles. Modifications to schedules are particularly vulnerable.

- (1) Delivery/pick-up schedules.
- (2) Dining hall schedules.
- (3) Distinguished visitor schedules.
- (4) Intelligence briefing schedules.
- (5) Laundry service schedules.
- (6) Leave schedule.
- (7) Personnel duty schedules.
- (8) Range schedules.
- (9) Religious service schedules.
- (10) Repair schedules.
- (11) Senior officer schedules/itineraries.
- (12) Test schedules.
- (13) Training schedules.
- (14) Transportation schedules.
- (15) Vehicle schedules.
- (16) Weekly duty rosters.

- (17) Weekly maintenance schedules.

C-6. PLANNING ACTIVITY INDICATORS.

a. Indicators establishing profiles.

- (1) Climatology.
- (2) Command control procedures.
- (3) Conferences.
- (4) Exercising.
- (5) Flight planning coordination.
- (a) Foreign overflight arrangements.

(b) International Civil Aviation Organization/Federal Aviation Administration filing/coordination.

- (c) Restricted airspace/ocean areas.
- (6) Force.
 - (a) Composition.
 - (b) Disposition.
 - (c) Pre-positioning.
- (7) Intelligence.
 - (a) Dissemination.
 - (b) Sources/methods.
 - (c) Gaps.
 - (d) Requirements.
- (8) Map and chart coverage.
- (9) Mission designators, codewords (single or double), codes numbers.
- (10) Number of aircraft/vehicles to participate.
- (11) Physical security upgrades on short notice, unusual priority.
- (12) Planned activity profile.

- (13) Reaction times/sequences.
- (14) Reconnaissance activities, ground and air.
- (15) Scenarios.
- (16) Sensor capabilities.
- (17) Spontaneous reactions.
- (a) Actions taken without communications.
- (b) Actions taken without coordination.
- (18) Strategy.
- (19) Tactics.
- (20) Testing.
- (21) Threat assumptions/intelligence.
- b. Indicators showing deviations.
 - (1) Actions taken without coordination/communication.
 - (2) Force augmentation.
 - (3) Pre-positioned forces/materiel/munitions/fuels.
 - (4) Rehearsals.
 - (5) Schedules modifications.
 - (6) Security augmentation.
 - (7) Unit activation.
 - (8) Weather limiting factors.

C-7. COMMAND AND STAFF ACTIVITY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Command control element.
 - (2) Command control procedures.
 - (3) Command control responses.

- (4) Commander's--
 - (a) Appearances in public.
 - (b) Health.
 - (c) Leave schedule.
 - (d) Personal affairs.
 - (e) Reactions under stress.
 - (f) Strategic and tactical behavior.
- (5) Commander/senior staff member identity.
- (6) Force composition.
- (7) Foreign or interagency liaison personnel.
- (8) Intelligence gaps.
- (9) Intercommand communications/coordination.
- (10) International communications flow.
- (11) Morale and discipline.
- (12) Organization structure.
- (13) Reactions to hostile actions.
 - (a) Reaction sequences.
 - (b) Reaction timing.
- (14) Reconnaissance activity.
- (15) Reconnaissance unit locations.
- (16) Staff officers'--
 - (a) Assignments.
 - (b) Experience.
 - (c) Skills and education.
- b. Indicators showing deviations.

- (1) Commander/senior staff itinerary.
- (2) Commander's leave schedule.
- (3) Deployment order.
- (4) Distinguished visitors.
- (5) Force command control.
- (6) Intelligence briefing subjects.
- (7) Organization restructuring.
- (8) Senior level interest.
- (9) Senior officer schedules.
- (10) Staff augmentation.
- (11) Subjects of intelligence emphasis.
- (12) Target damage assessments.
- (13) Unit orders.

C-8. COMMUNICATIONS ACTIVITY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Antenna types/orientation.
 - (2) Brevity codes.
 - (3) Call signs.
 - (4) Circuit/system requirements.
 - (5) Communications discipline.
 - (6) Communications-Electronics Operating Instructions (CEOI).
 - (7) Communicator signature feature.
 - (8) Encryption/encoding/authentication systems.
 - (a) Capabilities.
 - (b) Circuits where used.

- (c) Effective editions/changes dates.
- (d) Requirements.
- (9) Flow/volume/intensity.
- (10) Frequencies assigned.
- (11) Identification, friend or foe (radar)/selective identification features codes.
- (12) International communications.
- (13) Military Affiliate Radio System (MARS) communications.
- (14) Message delivery efficiency/speed.
- (15) Message formats.
- (a) Addressees.
- (b) Lengths.
- (c) Priorities.
- (16) Net/circuit designators.
- (17) Nets/net membership.
- (18) Nodes and choke points.
- (19) Operating restrictions.
- (20) Power requirements/sources.
- (21) Priorities.
- (22) Procedures to counter C3CM actions.
- (23) Radio check.
- (24) Reporting times.
- (25) Security classification.
- (26) Security procedures/authentication procedures.
- (27) Systems usage.
- (28) Technical studies.

- (29) Telephone usage.
- (30) Transmission signature features.
- b. Indicators showing deviations.
 - (1) Authentication requirements.
 - (2) Breakdowns in communications.
 - (3) C3CM hostile effectiveness.
 - (4) Communications degrades.
 - (5) CEOI modifications.
 - (6) Communications methods modification.
 - (7) Equipment changes/modification.
 - (8) Flight safety communications.
 - (9) Frequency changes.
 - (10) Frequency designators.
 - (11) Homemade codes.
 - (12) Personal communications.
 - (13) Radio silence.
 - (14) Rendezvous beacons.
 - (15) Routing indicator changes.
 - (16) Special capabilities/requirements.
 - (17) Station changes.
 - (18) Telephone service requests.
 - (19) Unofficial/personal call signs.
 - (20) Weather addressees/priorities.

C-9. ELECTRONIC ACTIVITY INDICATORS.

- a. Indicators establishing profiles.

- (1) Crypto system/secure usage.
 - (2) Communications clear to secure no change.
 - (3) Communications flow/volume standard.
 - (4) C3CM.
- b. Indicators showing deviations.
- (1) Countermeasures increase.
 - (2) C3CM increase.
 - (3) Decrease in normal clear traffic.
 - (4) Increase in secure net traffic.
 - (5) Strict procedural enforcement.
 - (6) Technical assisted nets increase.
 - (7) New nets/systems on unused frequencies.
 - (8) Weapons systems emissions strictly controlled.

C-10. SYSTEMS CAPABILITIES INDICATORS.

- a. Indicators establishing profiles.
- (1) Information system (automated data processing (ADP))--
 - (a) Use.
 - (b) Dependency.
 - (c) Alternatives.
 - (d) Security.
 - (e) Programming.
 - (f) Types/models.
 - (g) Capacities.
 - (h) Product flow/volume.
 - (i) Tempest status.

- (2) Modes of operations.
- (3) Nameplate data.
- (4) Operating instructions.
- (5) Physical security systems.
- (6) Reliability.
- (7) Security classification guides.
- (8) Technical studies.
- (9) Test equipment.
- b. Indicators showing deviations.
 - (1) Communication system deployments.
 - (2) Information system deployments.
 - (3) Modifications.
 - (4) Paint/preservative finishes.
 - (5) Performance degrades.
 - (6) Sensor system deployments.
 - (7) System-wide deficiencies/downgrades.
 - (8) Testing.

C-11. FINANCIAL ACTIVITY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Budget analysis.
 - (2) Budget justification statements and summaries.
 - (3) Budget projections and estimates.
 - (4) Budget requirements.
 - (5) Financial plans.
 - (6) Operating budgets.

- (7) TDY funds limits.
- (8) TDY funds requirements.
- b. Indicators showing deviations.
 - (1) Advance payments.
 - (2) Budget modifications.
 - (3) Budget supplements.
 - (4) Program objective memorandum inputs.
 - (5) System modification kit/component funding.
 - (6) TDY funding projected.
 - (7) TDY fund usage.
 - (8) Travel vouchers.
 - (9) Unplanned funding actions.
 - (10) Year-to-year comparisons.

C-12. LOGISTICS SUPPORT TRANSPORTATION INDICATORS.

- a. Indicators establishing profiles.
 - (1) Cargo/shipment.
 - (a) Classification.
 - (b) Identification numbers/codes.
 - (c) Number of pieces.
 - (d) Origin/routing/destination.
 - (e) Priority.
 - (f) Security classification.
 - (g) Weight/cubic feet.
 - (2) Commercial transport use.
 - (3) Courier service.

- (4) Materiel handling.
- (5) Modes of transport available/used.
- (6) Movement assembly areas.
- (7) Movement nodes/choke points.
- (8) Nuclear weapons/components procedures/routines.
- (9) Personal property shipments.
- (10) Requirements.
- (11) Specialized vehicles/aircraft.
- (12) Transportation control numbers.
- (13) Vehicle/aircraft capabilities.
 - (a) Identification.
 - (b) Number.
 - (c) Status.
 - (d) Type.
- (14) Vehicle/aircraft density.
- (15) Vehicle/aircraft movement activity.
- (16) Vehicle/aircraft schedules.
- b. Indicators showing deviations.
 - (1) Container labels.
 - (2) Convoy assembly.
 - (3) Delivery/pickup suspense dates.
 - (4) Munitions movement.
 - (5) Name tags.
 - (6) Personal luggage assembly.
 - (7) Resource movement.

(8) Travel authorizations.

(9) Travel reservations.

C-13. MAINTENANCE AND REPAIR ACTIVITY INDICATORS.

a. Indicators establishing profiles.

(1) Vehicle density/equipment density.

(2) Downtime planned for repairs/maintenance.

(3) Estimated time to completion of repair/maintenance.

(4) Equipment calibration.

(5) Equipment design features and nomenclature.

(6) Equipment nomenclature.

(7) Maintenance of prepositioned equipment.

(8) Rotation of stock items.

(9) Maintenance team movements.

(10) Maintenance activity routine.

(11) Maintenance trends.

(12) Materiel handling.

(13) Nuclear weapons/components procedures.

(14) COMSEC equipment allocations.

(15) System/element identification.

(16) Technical order changes.

(17) Technical studies.

(18) Test equipment.

(19) Repair scheduling.

b. Indicators showing deviations.

(1) Damage assessments.

- (2) Weapons systems modifications.
- (3) Equipment awaiting parts.
- (4) Equipment modifications.
- (5) Failure rates.
- (6) Quality control deficiencies.
- (7) Systems modification kits/components.
- (8) System-wide maintenance requirements/deficiencies.
- (9) Tool box shortages.
- (10) Test equipment shortages.
- (11) Change of priority of units.
- (12) Reallocation of critical items.
- (13) 24-hour maintenance/repair work.

C-14. MATERIEL ACQUISITION AND SUPPLY INDICATORS.

- a. Indicators establishing profiles.
 - (1) Camouflage.
 - (2) Classified stock number.
 - (3) Demineralized water.
 - (a) Capacity.
 - (b) Production rate.
 - (c) Requirements.
 - (d) Storage capacity.
 - (4) Fuels and lubricants.
 - (a) Full loads.
 - (b) Bulk storage records.
 - (c) On-hand/inventory.

- (d) Requirements.
- (e) Shipment/receipt.
- (f) Special types.
- (g) Storage capacity.
- (h) Supplier/source.
- (i) Transfer/refueling capacity.
- (5) Special lubricants and fuels.
 - (a) Capacity.
 - (b) Inventory.
 - (c) Records of use.
 - (d) Requirements.
 - (e) Resupply/source.
 - (f) Transfer rate/capacity.
- (6) Maps and charts.
 - (a) Availability/coverage.
 - (b) Production requirements.
 - (c) Overlays or special details.
 - (d) Requirements.
 - (e) Scale.
 - (f) Short titles/numbers.
- (7) Materiel delivery.
 - (a) Schedules.
 - (b) Suspense dates/times.
 - (c) Volumes.
- (8) Materiel handling.

- (9) Material pipelines, nodes, and chokepoints.
- (10) Mobility assets.
- (11) Munitions.
 - (a) Personal weapons/components.
 - (b) Crew-served weapons/components.
 - (c) Special weapons procedures.
- (12) Nameplate data.
- (13) Name tags.
- (14) Parts availability.
- (15) Personal equipment.
- (16) Provisions.
- (17) Provisions requirements/priorities.
- (18) Quantities on-hand/inventory.
- (19) Reliability of parts.
- (20) Requisition.
 - (a) Priorities.
 - (b) Procedures.
 - (c) Timing.
 - (d) Volume.
- (21) Shelf life times.
- (22) Stockpile conditions.
- (23) Storage capabilities.
- (24) Survival equipment.
- (25) Systems mod kits/components.
- (26) Test equipment.

- (27) Nuclear, biological, and chemical equipment.
- b. Indicators showing deviations.
 - (1) Equipment awaiting parts.
 - (2) Failure rates.
 - (3) Munitions movements.
 - (4) Pile-ups.
 - (5) Prepositioned materiel, fuels, munitions.
 - (6) Repair cycle assets.
 - (7) Requisition priorities.
 - (8) Specialized equipment.
 - (9) Staging of materiel.

C-15. PUBLIC RELATIONS AND PUBLIC NOTICE INDICATORS.

- a. Indicators establishing profiles.
 - (1) Background news articles and releases.
 - (2) Contractor advertisements.
 - (3) Legal/regulatory publications.
 - (4) Technical journal articles.
 - (5) Use of deadly force notices.
 - (6) Warning notices.
- b. Indicators showing deviations.
 - (1) Advertisements for bids.
 - (2) Advertisements for personnel hiring.
 - (3) Increased training activities.
 - (4) Environment impact statements.
 - (5) Hazardous testing or training notices.

- (6) Human interest/hometown news releases.
- (7) Restrictions on right-of-way through areas.
- (8) News releases.
- (9) Closing of post facilities, hunting, and fishing.
- (10) Posting of range firing and night operations.
- (11) Personnel hiring/layoffs.
- (12) Public appearances.

C-16. ENGINEERING AND SERVICE SUPPORT INDICATORS.

a. Indicators establishing profiles.

- (1) Maintenance and repair activities.
- (2) Billeting capacity/use.
- (3) Design factors.
- (4) Dining hall operations.
- (5) Utility requirements.
 - (a) Electric.
 - (b) Water.
 - (c) Heat.
- (6) Engineering studies.
- (7) Environmental impact statements.
- (8) Equipment availability/status.
- (9) Firefighting capabilities.
 - (a) Response time.
 - (b) Operations.
- (10) Laundry service capacity use.
- (11) Lighting.

- (12) Provisions.
- (13) Road usage.
- (14) Runway usage.
- (15) Structural capabilities/design.
- (16) Mobility team equipment.
- (17) Survival equipment services.
- (18) Technical studies.
- (19) Trash disposal.
 - (a) Disposal site.
 - (b) Schedule.
 - (c) Volume.
- (20) Unpaved road requirements/use.
- b. Indicators showing deviations.
 - (1) Billeting/services arrangements.
 - (2) Breakdowns.
 - (3) Camouflage.
 - (4) Damage assessments.
 - (5) Detectable pollutants.
 - (6) Environmental profile.
 - (a) Heat.
 - (b) Lighting.
 - (c) Smoke/chemical aerosols/smells.
 - (d) Sound.
 - (7) Motel/hotel reservations/contracts.
 - (8) New construction.

- (9) Road closures/degrades.
- (10) Structure modifications.
- (11) Work force scheduling.
- (12) Staging of mobility equipment.
- (13) Facility maintenance/usage.
- (14) Feeding schedules.

C-17. CIVIL GOVERNMENT AND COMMERCIAL SUPPORT INDICATORS.

- a. Indicators establishing profiles.
 - (1) Civilian facility use.
 - (2) Contract security and OPSEC specifications.
 - (3) Contract specifications.
 - (4) Memorandums of agreement.
 - (5) Technical studies and reports.
 - (6) Trash disposal.
- b. Indicators showing deviations.
 - (1) Commercial assistance requirements.
 - (2) Commercial personnel movement.
 - (3) Commercial manpower.
 - (4) Commercial movements of materiel.
 - (5) Courier service.
 - (6) Delivery/pickup locations and dates/times.
 - (7) Local government notifications.
 - (8) Local law enforcement coordination/support.
 - (9) Requests for proposals/bids.
 - (10) Technical representative visits.

- (11) Transportation support.
- (12) Traffic control.
- (13) Vehicle rental.
- (14) Telephone service requests.

GLOSSARY

ACofS	Assistant Chief of Staff
CEOI	Communications-Electronic Operating Instructions
CFC	Combined Forces Command
CINCPAC	Commander in Chief, Pacific
COMSEC	communications security
C2	command and control
C3	command, control, and communications
C3CM	command, control, and communications countermeasures
EEFI	essential elements of friendly information
IAW	in accordance with
MARS	Military Affiliate Radio System
MOS	military occupational specialty
NLT	not later than
OPSEC	operations security
ROK	Republic of Korea
TDA	tables of distribution and allowances
TDY	temporary duty
UNC	United Nations Command
US	United States
USAFK	United States Air Forces Korea
USFK	United States Forces Korea

유엔사/연합사/주한미군사 규정 530-1
제 1번경판

유엔사
사령부
부대번호 15259
군우 96205-0032

한미 연합사
사령부
부대번호 15255
군우 96205-0028

주한미군
사령부
부대번호 15237
군우 96205-0010

유엔사/연합사/주한미군사 규정
번호. 530-1
제 1번경판

작전 및 신호 보안

작전 보안(OPSEC)

1. 1990년도 7월 30일자 유엔사/연합사/주한미군사 규정 530-1은 하기와 같이 변경되었다:

1쪽, 제 3항, 참조. 1쪽 제 3항 나에서, “작전계획”단어 뒤에 마침표를 삽입하고 “우발 계획 및 작전 명령...별지 1”까지 나머지 문장 전체를 삭제한다. 유엔사/연합사/주한미군사 작전계획의 부록 다, 별지11, 부첨 다로 대체한다.

1쪽, 제 3항, 참조. 제 3항 마에서, 문장 전체를 삭제하고 하기와 같이 대체한다: 연합사/주한미군사 첩보작전(IO) 지침서.

2쪽, 제 5항, 책임. 제 5항 다(2)에서, 문장 맨 앞에 “필요시”라는 단어를 추가한다.

3쪽, 제 5항, 책임. 제 5항 다(5)에서, “, 개념계획 및 지시”를 삭제하고 “작전 보안 부록”뒤에, “및 유엔사/연합사/주한미군사 작전계획의 부록 다, 별지11, 부첨 다”를 삽입한다.

3쪽, 제 5항, 책임. 제 5항 마(1)에서, 둘째 줄의 “C3”을 삭제하고 “C2”로 대체한다.

유엔사/연합사/주한미군사 규정 530-1
제 1 변경판

4쪽, 제 5항, 책임. 제 5항 사(9)의 2째 줄에서, 정보참모부 보안과, 군사우편 샌프란시스코 96301-0010을 연합사·주한미군 작전참모부-계-첩보작전, 군우 96205-0010으로 변경한다.

5쪽, 제 6항, 일반적인 개념. 제 6항 다를 삭제한 후, 하기 내용으로 대체한다:
"작전 보안은 첩보작전(IO)의 주요 구성요소이다. 첩보작전(IO)은 전자전, 기만, 작전 보안, 컴퓨터망 공격, 심리전 작전, 공보, 민사 업무 및 물리적 파괴를 통합하여 적의 효과적인 지휘 및 통제를 거부하는 한편, 이와 유사한 적 활동으로부터 우군 C2를 보호하는 군사활동이다. 첩보작전(IO)의 한 분야로써, 작전 보안은 주요 비밀을 보호함으로써 평상시 적 결심권자에 영향을 준다. 적대 행위가 임박하거나 전투가 시작될 때, 작전 보안은 우군의 C2 능력을 보호하고, 기습 요소를 보존하며, 적에게 불확실성과 혼란을 가중시킨다."

5쪽, 제 6항, 일반 개념. 제 6항 마의 첫째 줄에서 지휘, 통제 및 통신 대책과를 첩보작전과로 변경한다.

6쪽, 제안자란. 제안자란의 마지막줄에서 "연작-계-대책, 군우 샌프란시스코 96301-0028"을 삭제한 후 "연작-계-첩보작전, 군우 96205-0010"으로 대체한다.

7쪽, 서명란, 별지. 별지 나를 "첩보작전(IO) 지원시 작전 보안"으로 변경한다.

7쪽, 배부선. 첫째 줄에서 연작-계-대책을 삭제한 후, 연작-계-첩보작전으로 대체한다. 배부선 내의 샌프란시스코를 모두 삭제한다.

별지 "가", 가-2 쪽. 제 4항 가(1)(마) 다음에 제 4항 가(1)(바), 컴퓨터 보안(인터넷 보안의식)을 첨가한다.

별지 "가", 가-2 쪽. 제 4항 가(2)에서 "지휘, 통제 및 통신 대책(C3CM)"을 삭제한 후, 첩보작전(IO)으로 대체한다.

별지 "나", 나-1 쪽. 제목에서 "C3CM"을 삭제한 후, "첩보작전(IO)"으로 대체한다.

별지 "나", 나-1 쪽. 제 1항의 3째 및 4째 줄에서 "지휘, 통제 및 통신(C3)"을 삭제한 후, 첩보작전(IO)으로 대체한다.

별지 "나", 나-1 쪽. 제 2항의 첫째 줄에서 2개의 C3CM을 모두 삭제한 후, 첩보작전(IO)으로 모두 대체한다.

별지 "나", 나-1 쪽. 제 2항 가의 첫째 줄에서 C3 대응책을 삭제한 후, 공세적 첩보작전(IO)으로 대체한다.

별지 "나", 나-1 쪽. 제 2항에서 하기사항을 변경한다:
제 2항 나1의 첫째 줄에서 C3 보호방책을 삭제한 후, 방어적 첩보작전(IO)으로 대체한다.
첫째 줄에서 C3 노드를 첩보작전(IO) 노드로 변경한다.

유엔사/연합사/주한미군사 규정 530-1

제 1 변경판

- 2째 줄에서 C3 보호를 방어적 첩보작전(IO)으로 변경한다.
- 3째 줄에서 C3 보호를 방어적 첩보작전(IO)으로 변경한다.
- 5째 줄에서 C3 보호를 방어적 첩보작전(IO)으로 변경한다.
- 5째 줄에서 C3 체계를 첩보작전(IO) 체계로 변경한다.
- 6째 줄에서 C3 대응책을 공세적 첩보작전(IO)으로 변경한다.

별지 "다", 다-14 쪽. 다-14 쪽의 (22)의 C3CM을 첩보작전(IO)로 변경한다.

별지 "다", 다-15 쪽. 다-15 쪽의 나(3)의 C3CM을 첩보작전(IO)로 변경한다.

별지 "다", 다-16 쪽. 다-16 쪽의 가(4)의 지휘, 통제 및 통신 대책(C3CM)을 첩보작전(IO) 대책으로 변경한다.

별지 "다", 다-16 쪽. 다-16 쪽의 나(2)의 C3CM을 첩보작전(IO)으로 변경한다.

약어. 약어에서 하기 사항을 변경한다.

C2와 C3 사이에 C2W, 지휘통제전을 첨가한다.

C3CM, 지휘, 통제 및 통신 대책을 삭제한다.

C4I, 지휘, 통제, 통신, 컴퓨터 및 정보를 첨가한다.

IAW, -에 의거 다음에 IO, 첩보작전을 첨가한다.

IO, 첩보작전 다음에 IW, 첩보전을 첨가한다.

2. 미 육군성 팸플렛 25-40에 의하여 본 변경사항을 게시한다.

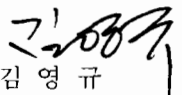
3. 본 변경사항을 출판물 앞에 삽입한다.

유엔사/연합사/주한미군사 규정 530-1
제 1 변경판

사용자는 의견 및 개선 제안사항을 미 육군성 양식 2028(출판물 및 백지 양식에 대한 수정
건의사항서)에 기재하여 유엔사/연합사 사령관(참조: CFCD-PL-IO, 군우 96205-0028)에
제출하기 바람.

유엔사/연합사 및 주한미군 사령관을 대신하여

주무관:
랜돌프 더블유. 하우스
미 육군 중장
참모장


김 영 규
한국육군 대령
유엔사/연합사 부관참모


존 에이. 홀
부관참모

특별 배부처:

- 25부 - 연작-계-첩보작전
- 2부 - 주한미군사령부 비서실
- 4부 - 주한미공군/7공군, 군우96570-5000
- 2부 - 주한미해군
- 2부 - 미8군 감찰부
- 1부 - 주한미군 공보실
- 1부 - 법무참모부
- 5부 - 주한미군 정보참모부
- 5부 - 주한미군 작전참모부
- 5부 - 주한미군 기획참모부
- 5부 - 주한미군 통전참모부
- 1부 - 미특수보안사령부, 태평양
- 1부 - 주한 미 야전 정보운영기지, 군우 96271-0161
- 15부 - 한미야전군사령부, 군우 96385-0210
- 15부 - 미 2 사단, 군우 96224-0289

유엔사/연합사/주한미군사 규정 530-1

제 1 변경판

- 5부 - 제 17 항공여단
- 2부 - 제 1 전투지원협조반, 군우 96397-0247
- 2부 - 제 3 전투지원협조반
- 15부 - 제 1 통신여단
- 4부 - 501 군사정보여단
- 1부 - 주한미국방성통신지국
- 2부 - 사령관, 태평양함대해병사령부, H. M. Smith 기지, 하와이, 군우 96861-5000
- 2부 - 미 제 5 공군사령부, 군우 96328-5000
- 2부 - 한국 공군 작전사령부
- 15부 - 3군 사령부
- 2부 - 한국해병대 사령부
- 5부 - 연합사 비서실
- 5부 - 연합사 정보참모부
- 5부 - 연합사 작전참모부
- 5부 - 연합사 기획참모부
- 5부 - 연합사 통전참모부
- 1부 - 미 수송사령부 연락장교
- 1부 - 연공보
- 2부 - 연운
- 2부 - 공군구성군사령부, 군우 96570-5000
- 2부 - 해군 구성군사령부, 진해, 한국
- 2부 - 유엔사 군사 정전위 사무국
- 2부 - 유엔사 군사 정전위원회 특별고문단
- 2부 - 유엔사 특별고문단
- 2부 - 유엔사 후방 사령부, Zama 기지, 일본, 군우 96343-0051
- 15부 - 1군 사령부
- 2부 - 한국군 합동 참모본부
- 4부 - 한국육군본부
- 4부 - 한국해군본부
- 4부 - 한국공군본부
- 1부 - 미 합동참모부/J3, 워싱턴, DC 20301-5000
- 4부 - 미 7함대 사령관, 군우 96601-5000
- 2부 - 미태평양사령부, H. M. Smith 기지, 하와이, 군우 96858-5000
- 2부 - 서부사령부, Shafter 기지, 하와이, 군우 96858-5000
- 2부 - 태평양공군사령부, Hickam 공군기지, 하와이, 군우 95853-5000
- 2부 - 미국방성주재, 미8군연락장교, 워싱턴, DC 20301-5000
- 2부 - 미태평양함대사령관, 진주만, 하와이 96818-5000
- 2부 - 제 3 상륙군, 군우 96606-5000
- 5부 - 연합특전사령부
- 2부 - 한국육군 항공사령부
- 3부 - 미 극동 물자사령부
- 90부 - 주한 미육군 인쇄창
- 8부 - 미 8군 통전참모부 출판 및 기록관리처 (편집)

유엔사/연합사/주한미군사 규정 530-1

유엔군사령부
군우 샌프란시스코 96301-0032

한미연합군사령부
서울, 한국
군우 샌프란시스코 96301-0028

주한미군사령부
군우 샌프란시스코 96301-0010

유엔사/연합사/주한미군 규정
530-1

1990년 7월 30일

(유효일자 1990년 8월 30일)
작전 및 신호 보안
작전 보안

증보. 유엔사/연합사령부, 참조: 연작-계-대책, 군우 샌프란시스코 96301-0028의
사전 승인없이 예하부대에 의한 본 규정의 증보를 금함.

1. 목적. 본 규정은 유엔사/연합사/주한미군사령부 및 예하사령부/참모부에게
작전 보안 방침과 지침을 제공하는데 있다.
2. 적용 범위. 본 규정은 유엔사/연합사 또는 주한미군사의 지원 또는 작전
통제하에 있는 예속 및 배속된 모든 인원과 부대에 적용된다.
3. 참조.
 - 가. 공군규정 55-30 (작전 보안)
 - 나. 유엔사/연합사 및 주한미군 작전계획, 우발계획 및 작전 명령 부록L 별지1
 - 다. 육군 규정 530-1 (작전 보안)
 - 라. 3군 합의각서
 - 마. 연합사/주한미군 지휘, 통제 및 통신 대책 (C3CM) 안내서

* 본 규정은 유엔사/연합사/주한미군 규정 530-1, 1980.6.23.의 대체임.

유엔사/연합사/주한미군 규정 530-1

바. 미합동참모부 발간물 3-54 (작전 보안 연합 교리)

사. J3M-947-83 (작전 보안 지침)

아. 해군 작전 지시 3070.1.A (작전 보안)

4. 약어 설명. 본 규정에서 사용된 약어는 용어 해석란에 설명되어 있음.

5. 책임.

가. 각 일반참모부 및 특별참모부는 작전 보안의 중요성을 강조하기 위해 자체 (처, 과, 반) 작전 보안 계획을 수립하여야 한다. 구체적인 참모 책임은 하기 "나"항 부터 "자"항 까지 명시되어 있다. 일반참모 및 특별참모는 최소한 아래 임무를 수행한다.

(1) 작전/계획 수립반에 작전보안장교를 임명하되 가급적 소령급이상 장교를 임명한다. 임명된 장교는 참모부의 작전 보안의 대표자로서 연합사/주한미군사 작전 보안 실무자 회의에 참가한다.

(2) 적이 연합사/주한미군사 작전 및 능력을 예지할수 있는 징후를 보호할수 있는 대책을 확인하고, 보호 우선순위를 수립하여, 방책을 발전시킨다.

(3) 연합사/주한미군사 작전보안장교 지시에 의거 임무를 수행한다.

나. 유엔사/연합사/주한미군사 C/J-2 :

(1) C/J-3가 우군 첩보 기본요소 작성시 이를 지원한다.

(2) 기만 기회를 확인한다.

(3) 필요시 기만계획에 필요한 자료를 제출 및 검토한다. 요구시 기만 임무를 수행한다.

(4) 적 정보 수집 위협 자료를 유지한다.

(5) 적 위협 수집 능력 및 의도를 분석한다.

(6) 우군부대 특징 작성시 이를 지원한다.

(7) 적의 정보 수집, 테러행위 및 태업에 대한 우군의 취약점을 확인한다.

다. 유엔사/연합사/주한미군사 C/J-3 :

(1) C/J-3 계획에 연합사/주한미군사 작전보안장교를 임명한다.

(2) 작전, 연습, 작전 보안 측정 및 평가, 훈련 및 지원이 포함된 작전 보안 활동에 필요한 예산을 편성한다.

유엔사/연합사/주한미군사 규정 530-1

(3) 구성군사와 예하부대 및 참모부에 작전 보안 관리, 계획 수립 및 실시 지침을 제공한다.

(4) 한국 국방부 및 미국방성 관계기관과 작전 보안을 협조한다.

(5) 연합사/주한미군 작전계획, 개념계획 및 지시에 필요한 작전 보안 부록 작성.

라. 유엔사/연합사/주한미군사 C/J-4 :

연합사/주한미군의 의도가 누설될수 있는 징후를 확인하기 위하여 군수 보고서 및 절차를 분석한다.

마. 유엔사/연합사/주한미군사 C/J-6 :

(1) 연합사/주한미군사 작전계획, 우발계획 및 연습 지시, C3 보호 부록을 작성한다.

(2) 연합사/주한미군 통신 및 비통신 방사체에 필요한 전파 방사 통제와 전시 운용 절차를 수립한다.

바. 유엔사/연합사/주한미군사 공병참모부 :

(1) 고정된 부대 시설과 시설물에 위장과 기만 형태를 적용시, 공사에 필요한 기술적인 조언을 실시한다.

(2) 필요시, 고정된 부대 시설과 시설물 설계 및 건축시에 대-감시 대책 통합 여부 상태를 확인한다.

사. 구성군사 및 예하사령부 :

(1) 작전참모부에 작전보안장교를 임명한다. 임명된 작전보안장교는 연합사/주한미군 작전 보안 실무자 회의시에 작전 보안 대표자로서 참석한다.

(2) 각급 제대는 부대 단위로 작전 보안 실무단을 구성한다. 참모들은 작전 보안 발전계획 수립과 실무자 토의에 적극적으로 참석한다.

(3) 연간 기준으로 작전 보안 활동에 필요한 예산을 편성한다.

(4) 작전계획, 연습계획 및 연습 지시, 작전 보안 부록을 작성한다.

(5) 예하부대에 및 참모부의 작전 보안 훈련 계획을 작성한다.

(6) 예하부대에 작전 보안 계획 지침 및 시행 지침을 제공한다.

(7) 요구시 연합사/주한미군사 작전 보안 측정팀 증원 요원을 지원한다.

(8) 연간 기준으로 우군 첩보 기본 요소(EEFI)를 작성 및 검토한다.

유엔사/연합사/주한미군사 규정 530-1

(9) 반기 작전 보안 평가 계획에 의거, 작전 보안 평가 요청을 수신:
연합사령관, 참조: 정보참모부 보안과, 군사 우편 샌프란시스코 96301-0010로
제출한다.

(10) 연간 작전 보안 활동 보고는 7월 15일까지 유엔사/연합사/주한미군사
작전보안장교에게 제출한다. 보고 양식은 6월 15일까지 유엔사/주한미군사로부터
전문으로 하달되며, 제7공군은 공군 규정 55-30과 태평양공군 지시에 의거 보고서를
제출한다.

(11) 장기간 업무로써 부대 작전 보안 현황을 작성한다.

아. 유엔사/연합사/주한미군사 작전보안장교 :

- (1) C/J-3로 부터 임무를 수령한다.
- (2) 예하부대에게 필요한 작전 보안 측정 및 평가 임무를 부여한다.
- (3) 합동 및 연합 작전 보안 능력을 발전시킨다.
- (4) 연합사/주한미군사 작전 보안 실무단을 구성한다.
- (5) 유엔사/연합사/주한미군사 작전 보안 장기 발전계획을 수립한다.
- (6) 유엔사/연합사/주한미군사 작전 보안 실무단 회의를 주최한다.
- (7) 연합사/주한미군사 주요 활동과 작전 보안 측정 상태를 감독한다.
- (8) 주한미군사 연간 작전 보안 활동 보고서를 8월 1일까지 태평양사령부로
제출한다.

자. 연합사/주한미군사 작전보안실무단은 필요시 다음과 같은 임무 수행을 위해
실무단 회의를 개최한다.

- (1) 작전 보안 계획 지시 및 시행사항을 검토 및 협조한다.
- (2) 정보 가치가 있는 추세, 징후, 형태 및 특징을 확인하기 위하여 부대
작전 보안 현황 및 참모의 작전 보안 측정 결과 보고서를 검토한다.
- (3) 유엔사/연합사/주한미군사 작전 보안 태세를 향상시킬수 있는 방안을
발전시킨다.
- (4) 취약한 징후를 보호할수 있는 대책과 기만 전술을 건의한다.
- (5) 취약한 징후를 보호할수 있는 대책과 기만 전술을 건의한다.
- (6) 사령부 작전 보안 활동 중점사항을 제공한다.
- (7) 작전 보안 평가 및 작전 보안 측정을 필요로 하는 작전을 건의한다.

6. 일반적인 개념.

가. 작전 보안은 적이 우군의 능력 및 의도에 관한 주요 첩보를 획득하지 못하도록 하는 과정이다. 우리는 군사 작전과 기타 군사 활동에 관련된 징후를 확인, 통제 및 보호함으로써 이와같은 작전 보안 임무를 수행한다. 징후에는 비밀 또는 비밀사항이 아닌 주요 첩보가 포함되어 있기 때문에 적은 우군의 작전 의도에 대응하고, 우군의 작전 효율성을 저하시키기 위해 이와같은 징후를 필요로 하고 있다. 유엔사/연합사 및 주한미군사 작전계획, 우발계획 및 작전 명령의 부록 "L" 별지1에 사령부의 주요 첩보가 포함되어 있다.

나. 작전 보안은 광범위하며, 정보, 기본적인 보안 군기 및 징후를 식별, 통제 및 보호하기 위한 참모 기능 분석

다. 작전 보안은 C3CM의 주요 구성요소이다. C3CM은 전자전, 기만, 작전 보안 및 물리적 파괴를 통합하여 적의 효과적인 지휘 및 통제를 거부하는 한편, 이와 유사한 적 활동으로부터 우군 C3를 보호하는 군사 활동이다. C3CM의 일분야로서, 작전 보안은 주요 비밀을 보호함으로써 평상시 적 결심권자에 영향을 준다. 적대행위가 임박하거나, 전투가 시작될때, 작전 보안은 우군의 C3 능력을 보호하고, 기습요소를 보존하며, 적에게 불확실성과 혼란을 가중시킨다.

라. 기만은 적에게 허위 정보들 누설하며 동시에 적의 정보 수집을 거부함으로써 군사 작전을 지원한다. 기만은 목적에 따라, 작전 보안을 지원하거나 또는 작전 보안 지원을 받는다. 작전 보안이 기만을 지원할때, 작전 보안은 우군 의도들 나타내는 징후를 최소화시키거나 또는 제거한다. 반대로 다른 대-감시 방책과 보호 기술을 사용할수 없거나 또는 불충분할때에는 기만을 작전 보안 대책으로 사용할수 있다. 작전 보안은 기만적인 의도없이 사용할수 있지만 기만은 효과적인 작전 보안 지원없이 성공할수 없다.

마. 유엔사/연합사/주한미군 작전보안장교는 C/J-3 계획처 지휘, 통제 및 통신 대책과에서 근무한다. 작전보안장교는 유엔사/연합사/주한미군사의 작전 보안 계획을 관리하고 태평양사령부, 합동참모본부 관계참모부와 구성군사 및 예하사령부 작전 보안장교와의 협조하에 작전 보안 임무를 수행한다.

바. 유엔사/연합사/주한미군사 작전 보안 목표에는 세가지가 있다.
첫째, 적이 이용할수 있는 첩보 출처의 수량을 감소시키고,
둘째, 적으로 하여금 한/미군의 의도, 목적 그리고 능력을 오인토록 유도하며,
셋째, 아군의 의도가 누설될수 있는 운용 방법을 대신할수 있는 방안을 개발한다.

7. 유엔사/연합사/주한미군사 작전 보안 방침.

가. 유엔사/연합사/주한미군사의 의도와 군사 능력에 관한 철저한 보안 유지는 대단히 중요한 관심사항이다. 효과적인 작전 보안은 중요한 비밀을 보호하고, 지휘관에게 기습을 실시할수 있는 수단을 제공하여 전장의 주도권을 장악하도록 한다.

나. 완전한 작전 보안 활동은, 연습기간뿐만 아니라 평상시 모든부대 활동을 통해서 실시하여야 한다.

다. 작전 보안은 지휘관의 책임이며 또한 지휘자의 책임사항이다. 구성군사와 예하부대 지휘관 및 참모는 적절한 작전 보안 대책을 일상적으로 적용함으로써 주요한 비밀을 보호하고 평상시의 부대 활동, 연습 또는 작전의 모든 단계에서도 작전 보안을 고려하여야 한다. 일상적인 참모 운용 절차, 보고 및 평상시 활동은 부주의로 인해 취약점을 노출시킬수 있다. 참모는 효율적인 작전 보안 대책을 적극적이고도 계획적으로 시행해야 하며, 이는 작전 보안 임무 수행에 대단히 중요하다.

라. 작전참모부는 작전 보안의 주무참모 책임을 수행하는 한편, 지휘관과 각 참모 부서장은 모든 예하부대 지휘관과 참모부서가 작전 보안을 모든 절차와 계획 수립 과정에 통합 작성하도록 해야 한다.

8. 작전 보안 지원 및 근무.

가. 제501정보여단 :

(1) J-2/J-3가 지정한 통신 체계에 대하여 위협 평가 및 위협을 분석한다.

(2) 통신 보안 장비 통제계획에 의거 전반적인 보안 태세를 확인하므로써 통신 보안 자재 보호상의 문제점과 영향을 확인/분석하기 위하여 주요 암호 자재를 보유하고 있는 암호 시설에 대한 검열을 실시한다.

(3) 기술 감시 장비, 위험도 및 시설 보안상의 취약점을 확인하기 위하여 기술적인 보안 감시 대책을 검사한다.

나. 6903 전자보안부대는 제7주한미공군 예하부대에 대한 통신 보안 감독 (유/무선 감청) 및 분석 지원 임무를 수행한다. 지역 45 특수보안담당관은 3군 근무 지원 협정에 의거 요청시 공군부대에 대한 기술 근무를 지원한다.

본 규정의 제안자는 작전참모부장입니다.

본 규정의 사용자들은 조언이나 개선사항이 있을때는 미육군성 양식 2028 (본 규정에 대한 변경 건의 내용 기록)이나 기타 적절한 서신을 통해 유엔사/연합사령부, 참조: 연작-계-대책, 군우 샌프란시스코 96301-0028로 발송해주시기 바랍니다.


유엔사/연합사/주한미군사 규정 530-1

유엔사/연합사 사령관을 대신하여 :


리차드 이. 카
미공군 소장
유엔사/연합사 참모장

주무관 :

제임스 알. 테일러
미육군 소장
주한미군사/미8군사 참모장



최 영 철
한육군 중령
유엔사/연합사 부관참모



조지 에프. 리브스
미육군 중령
주한미군사 부관참모

별지 3.
가. 작전 보안 훈련
나. C3CM 지원시 작전 보안
다. 작전 보안 징후

용어 해설

배부선 :
25 - 연작-계-대책
2 - 주한미군사령부 비서실
4 - 주한미공군/7공군, 군우 샌프란시스코 96570-5000
2 - 주한미해군
3 - 주한미합동군사지원단, 군우 샌프란시스코 96302-0187
2 - 미8군 감찰부
1 - 주한미군 공보실
1 - 법무참모부
5 - 주한미군사 정보참모부
5 - 주한미군사 작전참모부
2 - 주한미군사 기획참모부
8 - 주한미군사 통전참모부

유엔사/연합사/주한미군사 규정 530-1

- 1 - 미특수보안사령부, 태평양
- 1 - 751군사정보대대, 군우 샌프란시스코 96271-0161
- 15 - 한미야전군사령부, 군우 샌프란시스코 96385-0210
- 15 - 미2사단, 군우 샌프란시스코 96224-0289
- 5 - 제17항공여단
- 2 - 제1전투지원협조반, 군우 샌프란시스코 96397-0247
- 2 - 제3전투지원협조반
- 15 - 제1통신여단
- 4 - 501군사정보여단
- 1 - 주한미국방성통신지국
- 2 - 미태평양함대해병대, 캠프에이취 엠. 스미쓰, 하와이, 군우 샌프란시스코 06861-5000
- 2 - 미제5공군사령부, 군우 샌프란시스코 96328-5000
- 2 - 한국 공군 작전사령부
- 15 - 3군
- 2 - 한국 해병대사령부
- 5 - 연합사 비서실
- 5 - 연합사 정보참모부
- 5 - 연합사 작전참모부
- 5 - 연합사 기획참모부
- 5 - 연합사 통전참모부
- 1 - 미수송사령부 연락장교
- 1 - 연공보
- 2 - 연운
- 2 - 공군구성군사령부, 군우 샌프란시스코 96570-5000
- 2 - 해군구성군사령부, 진해 한국
- 2 - 유엔사 군사정전위 사무국
- 2 - 유엔사 군사정전위 특별자문단
- 2 - 유엔사 특별자문단
- 2 - 유엔사 후방지휘소, 캠프자마, 일본 군우 샌프란시스코 96343-0051
- 15 - 1군
- 2 - 한국 합참
- 4 - 한국 육군본부
- 4 - 한국 해군본부
- 4 - 한국 공군본부
- 1 - 미합동참모부/J3, 와싱턴 DC 20301-5000
- 4 - 미7함대사령부, 군우 샌프란시스코 96601-5000
- 2 - 미태평양사령부, 캠프 에이취 엠. 스미쓰 하와이 군우 샌프란시스코 96861-5000
- 2 - 서부사령부, 새프터 요새, 하와이, 군우 샌프란시스코 96858-5000
- 2 - 태평양공군사령부, 허캄 공군기지, 군우 샌프란시스코 96853-5000
- 2 - 미국방성주재 미8군연락장교, 와싱턴, DC 20301-5000
- 2 - 미태평양함대사령부, 진주만, 하와이 96818-5000
- 2 - 제3상륙군, 군우 샌프란시스코 96606-5000
- 5 - 연합특전사령부
- 2 - 한국 육군항공사령부
- 3 - 미국동물자사령부
- 90 - 주한미육군 인쇄창
- 8 - 주한미군 통전참모부 간행 및 기록관리처 간행물과

별지 "가"

작전 보안 훈련

1. 개요. 작전 보안 훈련 계획을 수립하여 실시하는 책임은 부대 지휘자와 작전 보안장교에게 있다. 작전 보안은 기초적인 사항으로써 전장에서 병사들의 생존성과 관련되어 있기 때문에 가장 상식적인 방법이 요구된다. 지휘자와 작전보안장교는 필수 과목 훈련시간을 확보하기 위해 기타 훈련 활동에 작전 보안을 통합 실시한다.

2. 목적.

가. 부대 훈련 계획을 수립/실시하는 목적은 적 위협 인식과 임무를 보호하는데 있다.

나. 위협 인식 훈련을 통하여 각 개인에게 적의 정보 수집 능력, 기술 및 제한사항을 교육시킨다.

다. 임무 보호 훈련은 가장 완전한 보호 수단으로 임무 수행 방법을 교육시킴으로써 적의 정보 수집 노력을 무력화시키는 것이다. 지휘자와 작전보안장교는 대상 인원 에 대한 세부 훈련 소요에 중점을 두고 여러단계에서 이와같은 훈련을 실시한다.

3. 위협 인지 훈련.

가. 효과적인 위협 인식 훈련은 부대의 특수 임무를 고려하여 계획된 훈련이다. 추가적으로 본 훈련은 적의 정보 수집 능력, 기술 및 제한사항을 고려하여 실시되어야 하며, 보안상 제한사항 및 정보 가용성은 허용 범위내에서 현실적이고 사실적이 되어야 한다.

나. 부대 작전 보안장교는 연합사/유엔사/주한미군사 정보참모부 관계장교와 협조하여 현행 적의 정보 위협과 브리핑 자료를 획득한다.

4. 안전 임무 수행 훈련.

가. 1단계 훈련은 모든 부대 구성원들이 작전 보안 원칙과 작전 보안이 기타 전통적 보안과 어떠한 관련성이 있는가에 대하여 이해하도록 한다. 모든 부대 요원은 국내 도착후 30일이내에 1단계 훈련을 받아야 한다. 보수 교육은 일상적인 활동과 적 정보 수집 활동 관계 즉 적에게 정보를 제공하는 출처와 발생할수 있는 결과를 보충 교육한다. 1단계 훈련 과제는 다음과 같다.

(1) 작전 보안과 기타 보안 계획간 상호 관계

(가) 자료 보안 (INFOSEC)

(나) 통신 보안 (COMSEC)

유엔사/연합사/주한미군사 규정 530-1

- (다) 전자 보안 (ELSEC)
- (라) 시설 보안
- (마) 전파 방사 통제 (EMCOM)
- (2) 작전 보안과 전술 기만 및 지휘, 통제 및 통신 대책 (C3CM) 간 상호관계.
- (3) 위장 및 대감시 훈련
 - (가) 개인 위장 기술
 - (나) 음영, 지형과 자연적인 위장기법을 적용한 군사 장비의 은폐
 - (다) 위장망의 적절한 운용법
 - (라) 차량 및 장비의 적절한 소산
 - (마) 방광, 방음 및 쓰레기 처리 군기
 - (바) 부대 통로 개척 계획의 발전
- (4) 대 - 신호 보안 훈련
 - (가) 통신망 통제
 - (나) 적절한 전화기 사용 기술
 - (다) 확인표 사용 절차
 - (라) 전자 보안 기술
 - (마) 수동식 암호 절차
 - (바) 주파수 및 호출부호 사용법
 - (사) 안테나 설치법
 - (아) 무선 침묵
 - (자) 무선/레이다 송신기의 최소 출력 사용
 - (차) 예비 통신 수단
 - (카) 약어표 사용 절차
 - (타) 무선 장비 정비 절차
 - (파) 보안 장비 키표 사용 절차

(5) 첩보 보안 훈련

- (가) 적절한 비밀 자료 취급 및 이관
- (나) 비문 분류 지침
- (다) 비문 자료 파기
- (라) 비밀 자료 재 생산

(6) 시설 보안 훈련

- (가) 지휘소 및 집결지 선정
- (나) 외곽 경계 설치
- (다) 암호호 사용 절차
- (라) 하차 지점 및 주차장 설치
- (마) 개인별 수색 절차

나. 2단계 훈련은 직접 및 간접적으로 비밀 문서 취급 또는 중요한 업무를 담당하고 있는 인원에게 필요한 훈련이다. 2단계 훈련 목적은 그들의 임무와 관련된 특정한 정보 징후를 인지할수 있는 능력을 개발하고 그와같은 징후가 우군 첩보 기본 요구서에 어떻게 반영되는가를 인식시키는데 있다. 각 개인은 이와같은 징후가 일단 확인될 경우, 징후 보호 방법을 숙지해야 한다. 징후는 특별한 활동 또는 작전에 따라서 변화될수 있지만, 그러나 일반적으로 두가지 범주 즉, 부대 능력 징후와 체제 개발, 시험 및 평가 능력 징후로 분류된다. 예상되는 징후 항목은 다음과 같다 :

(1) 능력

(가) 새로운 무기, 장비, 항공기, 절차 및 교리의 운용과 관련되는 관측 가능한 훈련/연습 활동

- (나) 연습 또는 실제적인 적대행위에 대한 반응
- (다) 예비 부품의 가용성
- (라) 인원의 훈련 및 경험 상태를 기술한 보고서
- (마) 주요 군사 특기 인원 현황을 기술한 보고서
- (바) 특수 수리 및 정비반 또는 민간 기술자의 방문

- (사) 장비/시설의 설치, 변경 및 수리
- (아) 이륙후 장비 점검
- (자) 정비 목록 부호
- (차) 부대 평가 및 연습 결과
- (카) 건설 및 수리 소요
- (타) 불리한 정비 추세 보고

(2) 체제 개발, 시험 및 평가 능력 징후

- (가) 시험 및 연습간 전파 방사 통제
- (나) 기술 잡지 및 보고서
- (다) 예산
- (라) 체제 개발
- (마) 시험 및 연습 실시 예정표
- (바) 시험을 지원하는 부대 및 감시 체제의 전개
- (사) 특별한 개발에 부여된 보안 조치
- (아) 시험에 필요한 인원 편성
- (자) 해군 및 공군요원에게 경고
- (차) 시험 준비를 위한 일정한 형태의 절차와 일련의 행동

다. 3단계 훈련은 참모부 계획 수립자들에게 필요한 훈련이다. 참모부 계획 수립자는 부대 계획, 명령 및 지시 작성시, 징후를 확인, 통제 및 제거하여야 한다. 참모부 계획 수립자는 또한 적 정보 수집 능력에 대한 기본적 이해와 작전 보안 원칙을 완전히 숙지하여야 한다. 훈련은 계획된 작전 또는 활동기간중 정상적인 활동과 예상된 활동의 비교에 중점을 두고 실시되어야 한다. 계획 수립자는 훈련시 다음사항을 고려하여야 한다.

- (1) 작전에 관련된 행동, 부대, 목적 또는 인원의 활동은 어떠한가?
정상적인 활동은 무엇인가?
- (2) 작전에 관련된 행동, 부대, 목적 또는 인원이 관측되는 장소는 어디인가?
이들이 정상적으로 관측되는 장소는?
- (3) 최초의 행동이 작전과 관련되는 시기는?
무엇이 정상인가?

- (4) 행동이 어느정도 작전과 관련되는가?
어느정도의 행동이 통상적으로 관련되는가?
- (5) 얼마나 많은 행동이 작전과 관련되는가?
얼마나 많은 행동이 통상적으로 관련되는가?
- (6) 행동이 몇번이나 작전과 관련되는가?
행동이 통상적으로 몇번이나 관련되는가?
- (7) 통상적인 활동과 관련사항을 비교할때 차이점, 이례적이거나 혹은
명백한 차이점은 무엇인가?
- (8) 이와같은 차이점에서 변동사항은 무엇인가?
차이점과 변동사항이 작전 징후가 될수가 있는가?

라. 4단계 훈련은 선임장교와 지휘관에게 필요한 훈련이다. 이들은 기습의 중요성을 이해하고 작전시 기습을 달성할수 있는 방법을 숙지해야 한다. 더우기 작전 보안이 이와같은 목적에 어떻게 기여하며, 작전 효율성과의 상호 관련성을 이해하여야 한다.

별지 "나"

C3CM 지원시 작전 보안

1. 개요. 규모에 관계없이 모든부대는 그들의 임무 수행을 위해 어떠한 형태의 지휘 및 통제가 필요하다. 통상적으로, 이와같은 지휘 및 통제는 통신과 밀접한 관계가 있고 또한 통신에 좌우된다. 지휘관은 지휘관 자신의 C3 체계를 동시에 보호하면서 적의 지휘, 통제 및 통신 체계를 분쇄할수 있다면 작전 성공 기회를 보다 크게 증대할수 있다.

2. C3CM 지원시 작전 보안. 효율적인 C3CM 전략은 적의 계획 수립자에게 중요한 첩보를 장기간 거부할수 있어야 한다. 적에게 완전하고, 정확한 첩보를 사용하여 계획을 수립할수 있도록 허용한다면, 교전중에 적은 그들의 통신 소요를 최소화할수 있을 것이다. 이와같은 현상은 적의 통신을 도청하거나 파괴, 전파 방해 또는 기만 방책을 사용하여 적의 결정 수립 과정을 교란시킬수 있는 아군의 기회를 감소시키게 된다.

가. C3 대응책 지원시, 효율적인 작전 보안 계획은 중요한 전술적 및 전략적 첩보를 차단한다. 전투시 결심권자의 실수는 치명적이 될수 있다. 결심 수립상의 착오는 부적절한 시간과 장소에서 부대를 비효율적으로 운영하는 결과를 초래할수 있다. 전투가 발전됨에 따라 적은 첩보를 상호 교환하고, 계획을 수정하며 부대를 재 전개하도록 강요를 받게 된다. 적의 첩보 상호 교환의 필요성 증가는 우군이 전파 방해, 기만 또는 파괴에 의한 방법을 이용하여 적의 능력을 저하시킬수 있는 기회를 증대시킨다.

나. C3 보호 방책 지원시, 작전 보안은 우군의 주요한 C3 노드, 통신망 구조와 운용 주파수를 필수적으로 보호한다. 전략 제대에서, 효율적인 C3 보호는 우군의 작전상 연구, 시험 및 개발 기능에 관련된다. C3 보호는 적으로 하여금 우군의 새로운 무기 체계를 파악하지 못하도록 하며, 우군이 기술적으로 기습을 달성할수 있는 요소가 된다. 빈약하게 계획되어 실시되는 C3 보호는 우군의 C3 체계가 적의 C3 대응책의 표적이 될때 작전상 효율성을 감소시키는 결함을 초래할수 있다.

별지 "다"

작전 보안 징후

1. 공통적인 징후

가. 부대 특징을 나타내는 징후

- (1) 출입자 연명부
- (2) 군수 물자 가용성
- (3) 회의 및 회합
- (4) 협조
- (5) 준비 태세 등급
- (6) 자료 처리 요소
- (7) 고정된 부대 활동 순서
- (8) 근무시간
- (9) 식별부호
 - (가) 약어/약성어
 - (나) 음어
 - (다) 임무 명칭
 - (라) 가명
 - (마) 사업 계획의 번호
- (10) 시행/실시 절차
- (11) 검사/평가/시험 결과
- (12) 상호 관련기관/국제간 협정
- (13) 부대의 능률을 저하시키는 요소
- (14) 부대/자원 위치
- (15) 부여된 임무
- (16) 핵 무기 운용 절차

유엔사/연합사/주한미군사 규정 530-1

- (17) 명령
- (18) 임무 수행 기준
- (19) 보직된 인원/참모 구성
- (20) 숙련도
- (21) 임무 수행 능력 통제
- (22) 보고/보고 절차
- (23) 소요
- (24) 제한된 활동사항
- (25) 보안 확인 및 시험
- (26) 비밀 취급인가 소요
- (27) 기호 특징 (활동/물자)
- (28) 자발적인 대응 행동 및 대응시간
- (29) 예규
- (30) 준비 태세

나. 비정상적인 활동을 나타내는 징후

- (1) 증원
- (2) 예비 자원/절차
- (3) 특수 집단/참모 소집
- (4) 중요 시간계획 조절
- (5) 결함/고장
- (6) 특별한 부대 기장 및 언어
- (7) 능률적인 수단
- (8) 비상 절차
- (9) 연습/예행 연습
- (10) 부대 자체에서 제작한 부호의 사용

- (11) 활동의 강도
- (12) 중요 어구의 사용
 - (가) "위급"
 - (나) "차상급 사령부"
 - (다) "지급"
 - (라) "긴급"
 - (마) "특수"
- (13) 위치
 - (가) 출발 지점/목적지
 - (나) 사전 배치된 자산
 - (다) 부대/자원
- (14) 계획 수립회의
- (15) 부여된 임무 우선순위
- (16) 근무 우선순위
- (17) 소요 변경
- (18) 긴급 소요
- (19) 보안 인식 및 경보
- (20) 비밀 취급인가 소요
- (21) 경계 증가
- (22) 결함 및 제한사항
- (23) 특수 소요
- (24) 시간/일자
 - (가) 도착/출발
 - (나) 이정표
 - (다) 마감 일자

(라) 적시성

(25) 근무 지원 요청/지원의 량

(26) 보안 위규

2. 행정 활동 징후

가. 부대 특징을 나타내는 징후

(1) 임무 기록 문서

(2) 행정적인 편성

(3) 행정 업무량

(4) 배부/수신처표시군 목록

(5) 문서 접수증

(6) 임무 및 직책 설명서

(7) 우편의 량

(8) 임무 설명서

(9) 운용 편성

(10) 작전 계획/작전 명령 수량

(11) 재산/재고품 영수증

(12) 발간물 수량/우선순위

(13) 비문 등급 분류

(14) 비문 분류 지침

(15) 편성 및 장비표, 분배 및 할당표, 편성 및 장비표 수정판 예규

나. 비정상적인 활동을 나타내는 징후

(1) 안전 사고/사건/재난 보고서

(2) 행정 서신

(3) 요청 양식

(4) 우편물 주소 변경

- (5) 우편물 발송
- (6) 보고서 배부
- (7) 비밀 취급 인가 요청
- (8) 보안 조사
- (9) 작업 명령/임무 요청

3. 개인 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 복장
- (2) 어린이 보호 근무
- (3) 교육 계획 참여
- (4) 면역 기록서
- (5) 세탁 근무
- (6) 신문 배달
- (7) 통행증
- (8) 개인 장비
- (9) 개인적인 계획
- (10) 개인적인 일상 생활
- (11) 개인 차량 표지
 - (가) 주둔지 표지
 - (나) 직책과 관련된 차량 표지
 - (다) 차량 번호판
 - (라) 주차 허가
- (12) 신체 검사/체력 측정
- (13) 개인용품 구매
- (14) 비밀 취급인가/출입

유엔사/연합사/주한미군사 규정 530-1

- (15) 배우자/부양 가족생활
- (16) 전화 근무/전화번호부
- (17) 부대 표지, 특수 기장

나. 비정상적인 활동을 나타내는 징후

- (1) 사전 지불
- (2) 숙식
- (3) 차량 대여
- (4) 수신인 주소 변경
- (5) 관사 입주/퇴거
- (6) 호텔/모텔 예약
- (7) 우편물 발송
- (8) 전속 명령
- (9) 부양 가족 정리
- (10) 개인 재산 정리
- (11) 개인 수하물
- (12) 대리 위임권(장)
- (13) 개인 주택 매매/임대
- (14) 보안 조사
- (15) 출장 명령
- (16) 휴가 중지
- (17) 여행 인가/증명서
- (18) 민간 교통 수단 이용
- (19) 유언

4. 인사 활동 징후

가. 부대 특징을 나타내는 징후

(1) 군사 주특기 소요

- (가) 보직 병력/계급별 병력 부족
- (나) 부대별, 분배 및 할당표
- (다) 주요 주특기 부족 현황
- (라) 부족

(2) 부대 현황

(3) 복장

(4) 막사 배열

(5) 부대 시험

(6) 부대 숙달 정도

(7) 장비/기술/상호 관련성

(8) 병력 보충 계획

(9) 의무/치과 진료 활동

(10) 사기 및 군기

(11) 명찰

(12) 인원 활동

(13) 개인 직무 예정표

(14) 신분

(15) 근무 위치

(16) 구금/재 입영

(17) 보안 감사

(18) 전문화 요원

(19) 참모장교 보직

- (20) 훈련 상태
- (21) 자격 숙달 정도
- (22) 훈련
- (23) 부대 표지
- (24) 부대 병력

나. 비정상적인 활동을 나타내는 징후

- (1) 사상자 보고서
- (2) 전개 명령
- (3) 교육 계획 수정
- (4) 면역 소요/기록
- (5) 이동 단계
- (6) 출입 금지지역
- (7) 인원 집결
- (8) 인원 고용/해고
- (9) 개인별 통보
- (10) 인원 소집
- (11) 신체 검사/체력 측정
- (12) 특수 기술 부족
- (13) 소화기 소유
- (14) 특수 인원 배치
- (15) 특수 기술 소요
- (16) 특수팀 전개/방문
- (17) 생존 훈련
- (18) 훈련 계획 수정
- (19) 출장비

유엔사/연합사/주한미군사 규정 530-1

- (20) 휴가 중지
- (21) 여행 승인/증명서
- (22) 여행 예약
- (23) 처벌 대상 인원 에 대한 첩보/처벌 행위
- (24) 부대 창설
- (25) 부대 비상

5. 예정표

예정표는 정상적인 활동 특성과 정상적인 활동 특성으로 부터 이탈된 행동 특성을 확인하는데 사용된다. 예정표의 수정은 특히 취약하다.

- 가. 배달/수령 예정표
- 나. 배식 시간표
- 다. 주요 인사 방문계획
- 라. 정보 브리핑 예정표
- 마. 세탁 근무 시간표
- 바. 휴가 계획
- 사. 개인 직무 예정표
- 아. 사격 시간표
- 자. 종교 행사 계획
- 차. 정비 예정표
- 카. 상급장교 업무 예정표/일정표
- 타. 테스트 예정표
- 파. 훈련 예정표
- 하. 수송 예정표
- 거. 차량 운행 예정표
- 녀. 주간 근무자 명단

더. 주간 정비 예정표

6. 계획 수립 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 기후
- (2) 지휘 통제 절차
- (3) 회의
- (4) 연습
- (5) 비행계획 협조
 - (가) 외국 항공기 상공 통과 협정
 - (나) 국제 민간항공기구/연방항공국 협정/협조
 - (다) 공중/해양 제한구역
- (6) 부대
 - (가) 구성
 - (나) 배치
 - (다) 사전 배치
- (7) 정보
 - (가) 전파
 - (나) 출처/방법
 - (다) 부족
 - (라) 소요
- (8) 지도 및 차트의 범위
- (9) 임무 명칭, 음어 (단일 또는 이중), 코드번호
- (10) 항공기/차량의 참가 수량
- (11) 단기 경고, 이례적이고도 우선적으로 취해진 시설 보안 강화 조치
- (12) 계획된 활동 특성

유엔사/연합사/주한미군사 규정 530-1

- (13) 반응시간/순서
- (14) 지상 및 공중 정찰 활동
- (15) 각본
- (16) 전자 정보 수집 장비의 능력
- (17) 자발적인 대응 행동
 - (가) 통신없이 취한 행동
 - (나) 협조없이 취한 행동
- (18) 전략
- (19) 전술
- (20) 시험
- (21) 위협 가정사항/정보

나. 비정상적인 활동을 나타내는 징후

- (1) 협조/통신없이 취한 행동
- (2) 부대 증원
- (3) 부대/군수품/탄약/연료의 사전 배치
- (4) 예행 연습
- (5) 예정표 수정
- (6) 경계 증원
- (7) 부대 창설
- (8) 기상 제한 요소

7. 지휘 및 참모 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 지휘 통제부대
- (2) 지휘 통제 절차
- (3) 지휘 통제 반응

(4) 지휘관의

- (가) 공식석상 참석
- (나) 건강
- (다) 휴가 예정표
- (라) 사생활
- (마) 긴장된 상황하에서의 반응
- (바) 전략적 및 전술적인 행동

(5) 지휘관/고위 참모 요원 신분

(6) 부대 구성

(7) 외국 연락장교 요원

(8) 정보 부족

(9) 통신/협조 상호간 지휘

(10) 국제 통신망 소통

(11) 사기 및 군기

(12) 편성

(13) 적대행위에 대한 대응 행동

- (가) 대응 순서
- (나) 대응 시간

(14) 정찰 활동

(15) 정찰부대 위치

(16) 참모장교

- (가) 보직
- (나) 경험
- (다) 숙달 및 교육

나. 비정상적인 활동을 나타내는 징후

유엔사/연합사/주한미군사 규정 530-1

- (1) 지휘관/선임참모장교 일일 행사표
- (2) 지휘관 휴가 예정표
- (3) 전개 명령
- (4) 주요 방문 인사
- (5) 부대 지휘 통제
- (6) 정보 브리핑 제목
- (7) 재 편성
- (8) 상급제대 관심
- (9) 선임장교 예정표
- (10) 참모요원 증원
- (11) 정보 활동 강화
- (12) 표적 피해 판단
- (13) 부대 명령

8. 통신 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 안테나 형태/방향
- (2) 약어표
- (3) 호출부호
- (4) 회선/체계 소요
- (5) 통신 군기
- (6) 통신-전자 운용 지시
- (7) 통신 신호 특성
- (8) 암호/조립/확인 체계
 - (가) 능력
 - (나) 사용 회로

- (다) 편집/변경 유효일자
- (라) 소요
- (9) 소통/소통양/농도
- (10) 할당된 주파수
- (11) 피아식별 (IFF/SIF) 코드
- (12) 국제간 통신
- (13) 군사 관련 무선 체계 (MARS) 통신
- (14) 전문 수발 능력/속도
- (15) 전문 양식
 - (가) 수신인
 - (나) 길이
 - (다) 우선순위
- (16) 통신망/회로 명칭
- (17) 통신망 가입자
- (18) 지역/주요 통신 확인소
- (19) 운용 제한사항
- (20) 전력 소요/전원
- (21) 우선순위
- (22) C3CM 대응 절차
- (23) 무선 점검
- (24) 보고 시간
- (25) 비밀 등급 분류
- (26) 보안 절차/확인 절차
- (27) 체제 사용법
- (28) 기술 연구 자료

(29) 전화 사용법

(30) 송신 신호 특성

나. 비정상적인 활동을 나타내는 징후

(1) 확인 소요

(2) 통신망 고장

(3) 적의 C3CM 효과

(4) 통신망 능력 감소

(5) 통신전자 운용 지시 수정

(6) 통신 방법 수정

(7) 장비 변경/수정

(8) 비행 안전 통신

(9) 주파수 변경

(10) 주파수 명칭

(11) 자대 제작 코드

(12) 사적인 통신

(13) 무선 침묵

(14) 집결지점 표지

(15) 노선 표지 변경

(16) 특수 능력/소요

(17) 통신소 변경

(18) 전화 근무 요청

(19) 비공식적인/개인적인 호출부호

(20) 기상 수신인/우선순위

다. 전자적인 활동 징후

가. 부대 특징을 나타내는 징후

유엔사/연합사/주한미군사 규정 530-1

- (1) 암호 체계/비화 체계 사용
- (2) 수정없이 평문 통화
- (3) 통신 소통/통화량
- (4) 지휘, 통제, 통신 대책

나. 비정상적인 활동을 나타내는 징후

- (1) 대응책 증가
- (2) C3CM 증가
- (3) 정상적인 평문 소통 감소
- (4) 비화 통신 증가
- (5) 엄격한 절차 사용 강조
- (6) 기술적으로 지원된 통신망 증가
- (7) 미사용된 주파수를 이용한 새로운 통신망/체계
- (8) 엄격하게 통제된 무기 체계의 전파 방사

10. 체제 능력 징후

가. 부대 특징을 나타내는 징후

- (1) 정보 처리 체제 (자동 자료 처리 체제)
 - (가) 운용
 - (나) 의존도
 - (다) 예비 운용 체제
 - (라) 보안
 - (마) 프로그램
 - (바) 종류/모델
 - (사) 능력
 - (아) 생산 자료의 유통/유통량
 - (자) 템페스트 보안 장비 현황

- (2) 운용 방식
- (3) 장비 명칭 자료
- (4) 운용 지시
- (5) 시설 보안 체계
- (6) 신뢰성
- (7) 비문분류 지침
- (8) 기술 연구 자료
- (9) 시험 장비

나. 비정상적인 활동을 나타내는 징후

- (1) 통신 체계 전개
- (2) 정보 체계 전개
- (3) 수정
- (4) 장비 도색/방부 처리 완료
- (5) 기능 저하
- (6) 감시 체계 전개
- (7) 체계의 광범위한 결함/기능 저하
- (8) 시험

11. 재정 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 예산 분석
- (2) 예산의 타당성 기술서 및 요약
- (3) 예산 계획/판단
- (4) 예산 소요
- (5) 재정적인 계획
- (6) 운용 예산

(7) 출장 자금 제한

(8) 출장 자금 소요

나. 비정상적인 활동을 나타내는 징후

(1) 사전 지불

(2) 예산 수정

(3) 예산 추가

(4) 계획 목표 각서 자료

(5) 장비 개조 키트/구성품 예산

(6) 계획된 출장 예산

(7) 출장 자금 사용

(8) 여행 증빙서

(9) 비예산 자금 활동

(10) 년도별 비교

12. 군수 지원 수송 징후

가. 부대 특징을 표시하는 징후

(1) 화물/선적

(가) 분류

(나) 확인 번호/부호

(다) 수량

(라) 출발 지점/노선/행선지

(마) 우선순위

(바) 비밀등급 분류

(사) 중량/용적

(2) 민간 교통 사용

(3) 전령 근무

- (4) 물자 취급
- (5) 가용/운용 수송 방식
- (6) 이동 집결지역
- (7) 이동 경로/애로 지점
- (8) 핵 무기/구성품 관리 절차/일과
- (9) 개인 물품 선적
- (10) 소요
- (11) 특수 차량/항공기
- (12) 교통 통제번호
- (13) 차량/항공기 능력
 - (가) 식별
 - (나) 수량
 - (다) 현황
 - (라) 형태
- (14) 차량/항공기 밀도
- (15) 차량/항공기 이동 활동
- (16) 차량/항공기 예정표

나. 비정상적인 활동을 나타내는 징후

- (1) 용기 표찰
- (2) 호송 집결지
- (3) 송달/수령 마감일자
- (4) 탄약 이동
- (5) 명찰
- (6) 개인 사물 집결지
- (7) 자원 이동

(8) 여행 인가

(9) 여행 예약

13. 정비 및 수리 활동 징후

가. 부대 특징을 나타내는 징후

(1) 차량 밀도/장비 밀도

(2) 수리/정비를 위한 장비 휴지기간

(3) 수리/정비 완료 예상시간

(4) 장비 구경 측정

(5) 장비 설계 특성 및 품명

(6) 장비 명칭

(7) 사전 비축 장비의 정비

(8) 저장 보급품 순환

(9) 정비팀 이동

(10) 정비 활동 일과

(11) 정비 추세

(12) 물자 취급

(13) 핵 무기/구성품 관리 절차

(14) 통신 보안 장비 배당

(15) 체제/부대 식별

(16) 기술 작업 명령서 변경

(17) 기술 연구 자료

(18) 시험 장비

(19) 수리 예정표

나. 비정상적인 활동을 나타내는 징후

(1) 피해 판단

- (2) 무기 체제 개조
- (3) 부품 대기 장비
- (4) 장비 개조
- (5) 고장 비율
- (6) 품질 통제 결함
- (7) 장비 개조기구/구성품
- (8) 체계 - 정비 소요/결함
- (9) 정비 도구 부족
- (10) 시험 장비 부족
- (11) 부대 우선순위 변경
- (12) 주요 품목 재 할당
- (13) 24시간 정비/수리 업무

14. 물자 획득 및 보급 징후

가. 부대 특징을 나타내는 징후

- (1) 위장
- (2) 재고번호 분류
- (3) 식수 (광물질이 포함되지 않음)
 - (가) 용량
 - (나) 생산 비율
 - (다) 소요
 - (라) 저장 용량
- (4) 연료 및 윤활유
 - (가) 최대 용량
 - (나) 저장 기록서
 - (다) 현 보유량/재고

- (라) 소요
- (마) 선적/수령
- (바) 특수한 형태
- (사) 저장 용량
- (아) 보급부대/출처
- (자) 수송/재공유 용량
- (5) 특수 유허유 및 연료
 - (가) 용량
 - (나) 재고
 - (다) 사용 실적 기록서
 - (라) 소요
 - (마) 재 보급/출처
 - (바) 수송 비율/용량
- (6) 지도 및 차트
 - (가) 가용성/범위
 - (나) 생산 요소
 - (다) 투명지 또는 특수 세부 항목
 - (라) 소요
 - (마) 규모
 - (바) 소 제목/번호
- (7) 물자 보급
 - (가) 예정표
 - (나) 보급 마감일자/시간
 - (다) 수량
- (8) 물자 취급

- (9) 물자 보급로 중요지점 및 애로지점
- (10) 기동 자산
- (11) 탄약
 - (가) 개인 화기/구성품
 - (나) 공용 화기/구성품
 - (다) 특수 화기 절차
- (12) 장비 제원 기록판
- (13) 장비 명찰표
- (14) 부품 가용성
- (15) 개인 장비
- (16) 식량
- (17) 식량 소요/우선순위
- (18) 보유량/재고
- (19) 부품의 신뢰성
- (20) 청구
 - (가) 우선순위
 - (나) 절차
 - (다) 시기
 - (라) 수량
- (21) 보관 유효기간
- (22) 저장 상태
- (23) 저장 용량
- (24) 구명 장비
- (25) 장비 개조 키트/구성품
- (26) 시험 장비

(27) 화생방 장비

나. 비정상적인 활동을 나타내는 징후

- (1) 부품 대기 장비
- (2) 고장율
- (3) 탄약 이동
- (4) 물자의 비축
- (5) 군수 물자, 연료 탄약 사전 비축
- (6) 수리 (주기) 자산
- (7) 청구 우선순위
- (8) 특수 장비
- (9) 군수 물자 집결

15. 공보/홍보 활동 징후

가. 부대 특징을 나타내는 징후

- (1) 주요 배경의 신문 기사화/보도
- (2) 계약 광고
- (3) 법률/규정 발간
- (4) 기술 잡지 기사
- (5) 위험 표지판 사용
- (6) 경고문 게시

나. 비정상적인 활동을 나타내는 징후

- (1) 입찰 공고
- (2) 고용인 모집 공고
- (3) 증가된 훈련 활동
- (4) 환경 영향 설명서
- (5) 위험한 시험 또는 설명서

유엔사/연합사/주한미군사 규정 530-1

- (6) 흥미 기사/고향 소식 공고
- (7) 지역 통과 진로권 제한
- (8) 뉴스 공개
- (9) 시설물, 사냥 및 낚시터 폐쇄
- (10) 사격, 야간 훈련 발표
- (11) 고용/해고
- (12) 공식 행사

16. 공병 및 근무 지원 징후

가. 부대 특징을 나타내는 징후

- (1) 정비 및 수리 활동
- (2) 숙소 수용 능력/사용
- (3) 설계 요소
- (4) 식당 운용
- (5) 시설물 소요
 - (가) 전기
 - (나) 급수
 - (다) 난방
- (6) 기술 연구 문서
- (7) 환경 영향 설명서
- (8) 장비 가용성/현황
- (9) 소방 능력
 - (가) 반응시간
 - (나) 운용
- (10) 세탁 용량
- (11) 조명

- (12) 식량
- (13) 도로 사용
- (14) 활주로 사용
- (15) 구조상 능력/설계
- (16) 이동팀 장비
- (17) 구명 장비 지원
- (18) 기술 연구 자료
- (19) 쓰레기 처리
 - (가) 처리 장소
 - (나) 시간표
 - (다) 분량
- (20) 비포장도로 소요/사용

나. 비정상적인 활동을 나타내는 징후

- (1) 숙소/근무 지원 시설 배치
- (2) 고장
- (3) 위장
- (4) 피해 평가
- (5) 탐지 가능한 오염 물질
- (6) 환경 특성
 - (가) 난방
 - (나) 조명
 - (다) 연기/화학적인 에어레졸/냄새
 - (라) 음향
- (7) 모텔/호텔 예약/계약
- (8) 신규 건설

유엔사/연합사/주한미군사 규정 530-1

- (9) 도로 폐쇄/파손
- (10) 구조물 변경
- (11) 민간 고용인 작업시간
- (12) 기동 장비 집결
- (13) 시설 정비/사용
- (14) 급식 계획

17. 정부/민간 지원 징후

가. 부대 특징을 나타내는 징후

- (1) 민간 시설 사용
- (2) 계약 보안 및 작전 보안 명세서
- (3) 계약 명세서
- (4) 합의각서
- (5) 기술 연구 및 보고서
- (6) 쓰레기 처분

나. 비정상적인 활동을 나타내는 징후

- (1) 민간 지원 소요
- (2) 민간인 이동
- (3) 민간 인력
- (4) 민간 군수 물자 수송
- (5) 전력
- (6) 발송/수령 위치 및 일자/시간
- (7) 현지 정부기관 통보
- (8) 현지 법률 시행 협조/지원
- (9) 제안/입찰 요청
- (10) 기술자 방문

유엔사/연합사/주한미군사 규정 530-1

- (11) 수송 지원
- (12) 교통 통제
- (13) 차량 대여
- (14) 전화 근무 요청

약어 설명

ACofS	참모
CEOI	통신전자 운용 지시
CFC	한미연합군사령부
CINCPAC	미태평양지구사령관
COMSEC	통신 보안
C2	지휘 및 통제
C3	지휘, 통제 및 통신
C3CM	지휘, 통제 및 통신 대책
EEFI	우군 첩보 기본 요소
IAW	-- 에 의거
MARS	군가입 아마추어 무선 체계
MOS	군사 주목기
NLT	- 이내까지
OPSEC	작전 보안
ROK	대한민국
TDA	분배 및 할당표
TDY	출장
UNC	유엔군사령부
US	미국
USAFK	주한미공군
USFK	주한미군